Appendix A
Organizational Summaries

Appendix A Organizational Summaries

APPENDIX A
TABLE OF CONTENTS

Note: Organizational summaries have not been completed for these organizations. The organization is included in the index for possible future review.

TABLE OF CONTENTS (Continued)

Note: Organizational summaries have not been completed for these organizations. The organization is included in the index for possible future review.

TABLE OF CONTENTS (Continued)

Organization Page

Independent Establishments and Government Corporations

Legislative and Judicial

International

National

Public Organizations

Note: Organizational summaries have not been completed for these organizations. The organization is included in the index for possible future review.

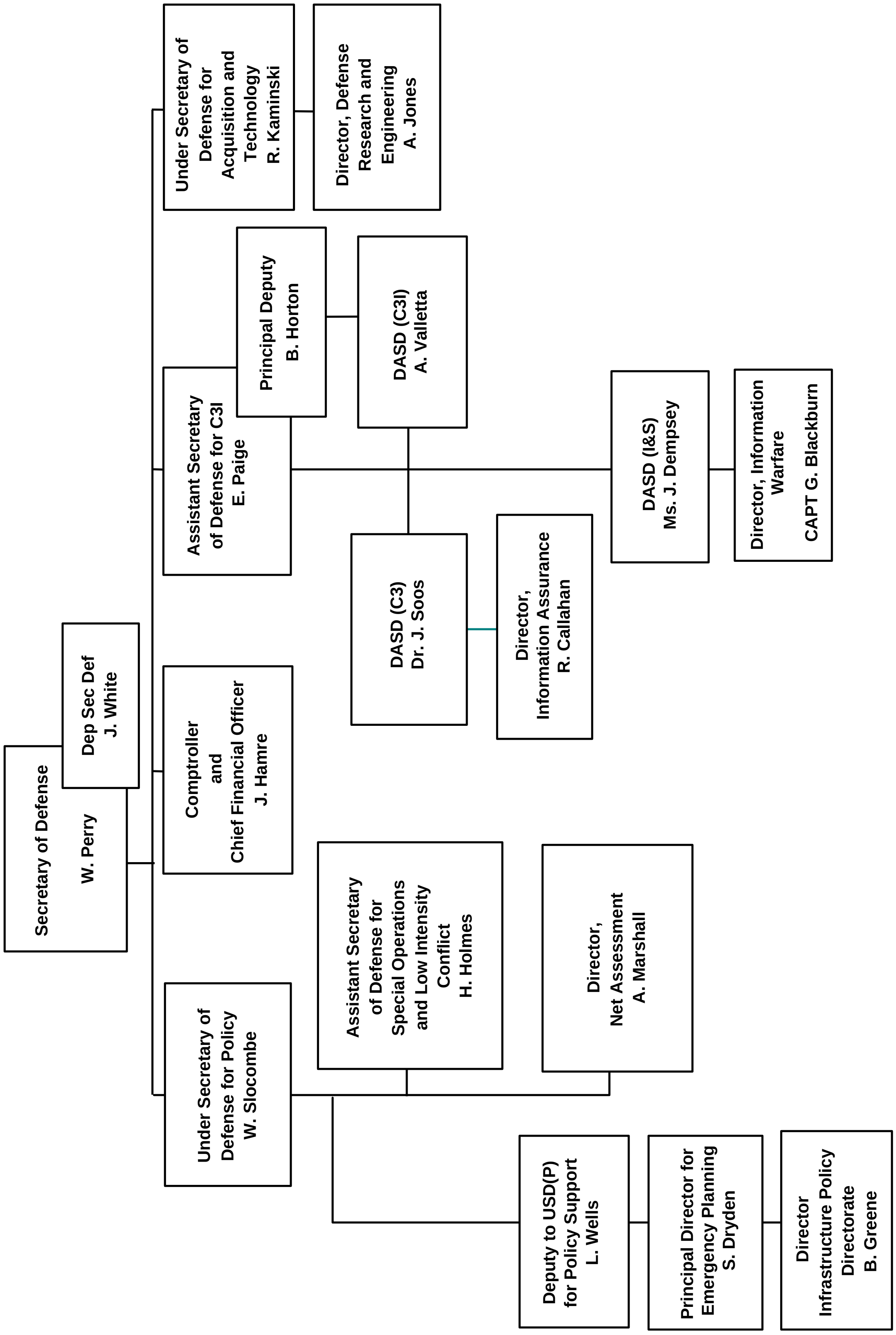
TABLE OF CONTENTS (Continued)

Note: Organizational summaries have not been completed for these organizations. The organization is included in the index for possible future review.

Department of Defense

Department of Defense

This page intentionally left blank.


Secretary of Defense
W. Perry
Dep Sec Def
J. White
Under Secretary of Defense for Policy
W. Slocombe
Comptroller and Chief Financial Officer
J. Hamre
Assistant Secretary of Defense for C3I
E. Paige
Principal Deputy
B. Horton
Under Secretary of Defense for Acquisition and Technology
R. Kaminski
Director, Defense Research and Engineering
A. Jones
DASD (C3I)
A. Valletta
DASD (C3)
Dr. J. Soos
Director, Information Assurance
R. Callahan
DASD (I&S)
Ms. J. Dempsey
Director, Information Warfare
CAPT G. Blackburn
Assistant Secretary of Defense for Special Operations and Low Intensity Conflict
H. Holmes
Director, Net Assessment
A. Marshall
Deputy to USD(P) for Policy Support
L. Wells
Principal Director for Emergency Planning
S. Dryden
Director Infrastructure Policy Directorate
B. Greene

Organization: Office of the Assistant Secretary of Defense (C3I)

Senior Information Assurance Official:

Emmett Paige, Assistant Secretary of Defense (C3I)

Information Assurance Points of Contact:

Roger Callahan, Director, Information Assurance
Captain Greg Blackburn, USN, Director, Information Warfare

On-Line Resources:

OASD(C3I) Homepage: http://www.dtic.dla.mil/defenselink/pubs/ofg/of_asdc3i.html

Information Assurance Related Missions and Functions:

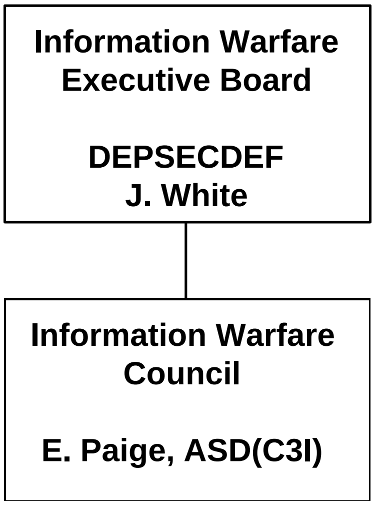
The ASD(C3I) has established a Directorate for Information Warfare to help the ASD(C3I) execute his task as the senior Information Warfare advisor to the Secretary of Defense and senior policy official in the Department for Information Warfare.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- OMB has an Information Security Oversight Organization which was created under the provisions of Executive Order (EO) 12356, National Security Information.
- Current version of the Paperwork Reduction Act exempts DoD and intelligence activities from certain provisions for OMB oversight. Revision to Act may not provide these exemptions.
- Vulnerability of nation to information disasters is generally accepted. It is not clear what the responsibilities should be for dealing with the issues.
- The ASD(C3I) has requested an Intelligence Community Assessment and National Intelligence Estimate of the foreign Information Warfare threat with emphasis on the physical threat to the infrastructure supporting the Public Switched Network and the electronic threat to the information present on and accessible through the network. The assessment was published in July 1995. It is expected the National Intelligence Estimate will be completed in late 1996 or early 1997.
- The ASD(C3I) sponsored an executive forum in January, 1995, to discuss critical Information Warfare issues facing the DoD.

- The ASD(C3I) is revising the current DoD Directive 3600.1, Information Warfare, to reduce the classification and, thereby, increase knowledge and awareness of the Department's policy and responsibilities for IW.
- The ASD(C3I) is supporting an active Red Team effort with the USD (A&T).
- The ASD(C3I) has developed and is coordinating a formal "Defensive Information Warfare Strategy."
- The ASD(C3I) and the President, National Defense University are exploring ways for the NDU to assume a central role in Information Warfare education and awareness.
- The USD(P) Office of Net Assessment and the ASD(C3I) have initiated a "Net Assessment of Information Warfare" as suggested by the Defense Science Board's 1994 Summer Study. Phase I of this Net Assessment will be completed by August 1996.
- The new Defense Planning Guidance (DPG) contains specific reference to enhancing Defensive Information Warfare/Information Assurance programs.
- The Deputy Secretary has established and will chair an Information Warfare Executive Board, supported by an IW Council. (See separate organizational summary for the IEWB.)
- The Deputy Secretary sponsored several "The Day After ..." games for members of his Executive Board and has invited members of the NSTAC Industry Executive Subcommittee, as well as other industry representatives to participate.
- The Deputy Secretary's IW Executive Board and ASD(C3I)'s Council will sponsor additional seminars, topical forums, and other events to bring the Department together with interested parties outside the Department to address critical Information Assurance issues.
- OASD(C3I) consider the past year a very successful year from the IW-D perspective:
    - Signing of PDD 39 and the creation of the Critical Infrastructures Working Group demonstrates high-level interest in infrastructure assurance.
    - A National HUMINT Directive has been published.
    - An Information Warfare Net Assessment is being conducted by OUSD(P)/NA.
    - USEUCOM deployed an operational IW-D team to Bosnia.
    - The Joint Command and Control Warfare Center has been exercising its Red Team capabilities.
    - Numerous CINC exercises and wargames provided many insights into tactics, doctrine, policy and organizational issues.
    - People are recognizing the need to share sensitive information -- offensive and defensive arms, intelligence and counter-intelligence, intelligence and operations.
    - Joint policy documents have been and are being published.
    - A Joint Mission Need Statement for Infrastructure Assurance Modeling has been coordinated by the Joint Staff (J6).
- OASD(C3I) initiated the Highlands Group to provide advice to the ASD(C3I) in information warfare concepts and their potential for revolutionary impact on DoD operations.

This page intentionally left blank.


Information Warfare
Executive Board
DEPSECDEF
J. White
Information Warfare
Council
E. Paige, ASD(C3I)

Organization: Information Warfare Executive Board (IWEB)

Senior Information Assurance Official:

John White, Deputy Secretary of Defense, Chairman

Information Assurance Points of Contact:

Emmett Paige, Assistant Secretary of Defense (C3I)
Captain Greg Blackburn, Executive Secretary, Director of Information Warfare, OASD(C3I)

On-Line Resources:

Information Assurance Related Missions and Functions:

The purpose of the Board is to provide a forum for the discussion and advancement of information warfare strategies, operations, and programs involving the Department of Defense.

The board is chartered to:

Provide advice and recommendations to the DEPSECDEF and to the ASD(C3I) in his capacity as the DoD Information Warfare Manager.

Provide for integrated development and consideration of IW policy, strategy, vulnerabilities and capabilities in all DoD activities, including formulation of IW recommendations for inclusion in the National Military Strategy, Defense Planning Guidance, and Contingency Planning Guidance.

Eliminate gaps, identify overlaps, and ensure reciprocity in IW programs and operations.

Serve as the forum for establishing coordinated DoD positions and recommendations on IW programs and operations, including interagency policy and strategy.

Serve as the focal point for discussion of DoD IW policy, capabilities, and equities with national agencies, including recommending IW issues for consideration in the National Security Strategy.

Improve participation of DoD corporate IW expertise and interests in the areas of policy, operations, intelligence, communications, and acquisition, both within the Department and at the national level.

Focus Department and national level information warfare strategy, capitalizing on information technology to accomplish national security goals and objectives.

Foster the development of training in IW concepts of operation, methodologies, potential vulnerabilities, and strategies for DoD and other national level entities.

Recommend new, or adjusted, DoD resource allocations consistent with IW policies and strategies.

Review plans and programs to ensure capabilities under consideration effectively and efficiently support IW policies and strategies.

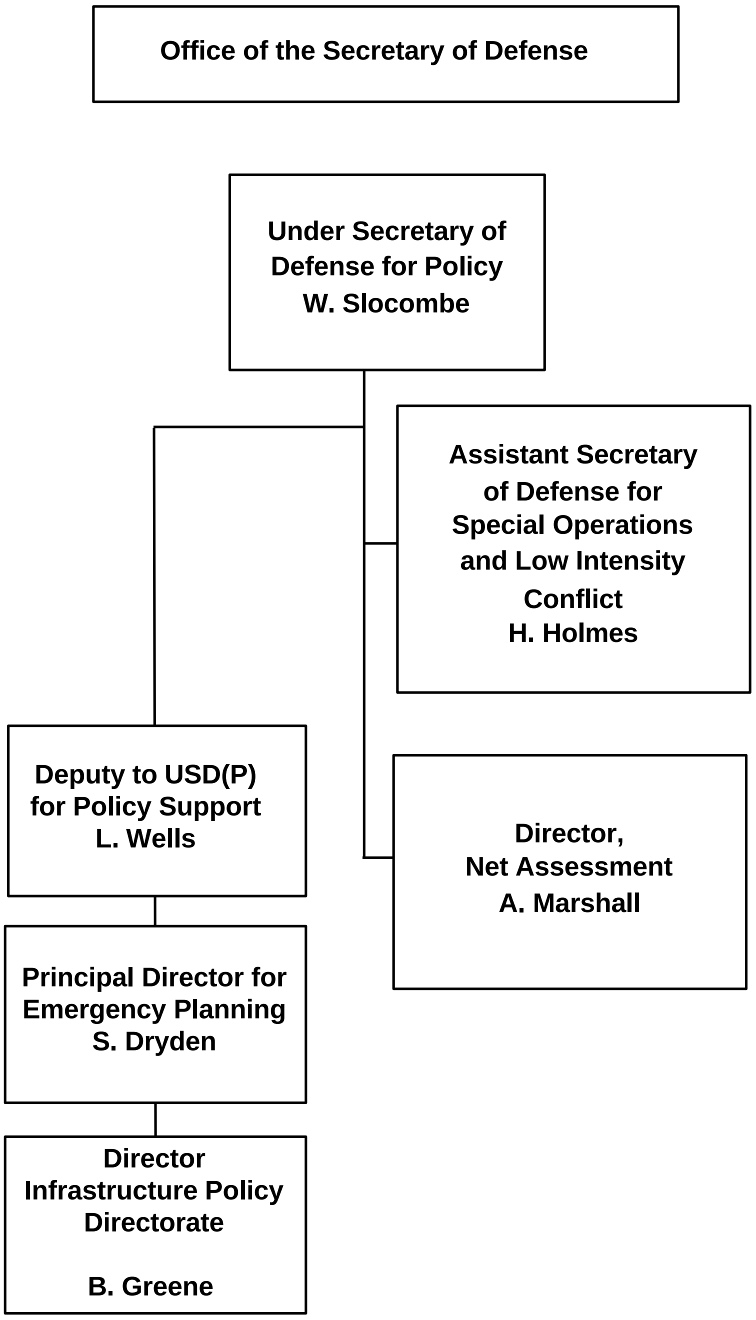
Membership of the IWEB includes:

Deputy Secretary of Defense (Chair)
Under Secretary of Defense (Acquisition and Technology)
Under Secretary of Defense (Policy)
Under Secretary of Defense (Comptroller)
Under Secretary of Defense (Personnel and Readiness)
Vice-Chairman, Joint Chiefs of Staff
Assistant Secretary of Defense for Command, Control, Communications and Intelligence
General Counsel of the Department of Defense
Vice Chiefs of the Military Services
Director, National Security Agency
Director, Defense Intelligence Agency
Director, Defense Information Systems Agency
Director, Program Analysis and Evaluation
Director, Information Warfare (Executive Secretary)
Deputy Director of Central Intelligence
Executive Director of the Central Intelligence Agency
National Security Council Executive

The IW Executive Board has a supporting Information Warfare Council (IWC) which will supervise supporting work for the Board. The IWC is composed of representatives designated by the IWEB representatives. The IWC also includes the Director of Special Programs, OUSD(A&T) and the Director of Net Assessment. Secretariat support for the IWEB and the IWC is provided by OASD(C3I). Other representatives from the Federal government may be invited to attend meetings as appropriate.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Board will serve as the DoD focal point for IW discussion at the National level.
- The OASD(C3I) is exploring the establishment of an Information Assurance Group which will be subordinate to the IWC and will coordinate the ad hoc working groups being established to address IW issues such as threat, threat assessments, and indications and warning.


Office of the Secretary of Defense
Under Secretary of Defense for Policy W. Slocombe
Assistant Secretary of Defense for Special Operations and Low Intensity Conflict H. Holmes
Deputy to USD(P) for Policy Support L. Wells
Director, Net Assessment A. Marshall
Principal Director for Emergency Planning S. Dryden
Director Infrastructure Policy Directorate B. Greene

Organization: Infrastructure Policy Directorate, Office of the Under Secretary of Defense (Policy)

Senior Information Assurance Official:

Linton Wells, Deputy to the Under Secretary of Defense (Policy) for Policy Support

Information Assurance Points of Contact:

Sheila Dryden, Principal Director for Emergency Preparedness Policy
Brent Greene, Director for Infrastructure Policy

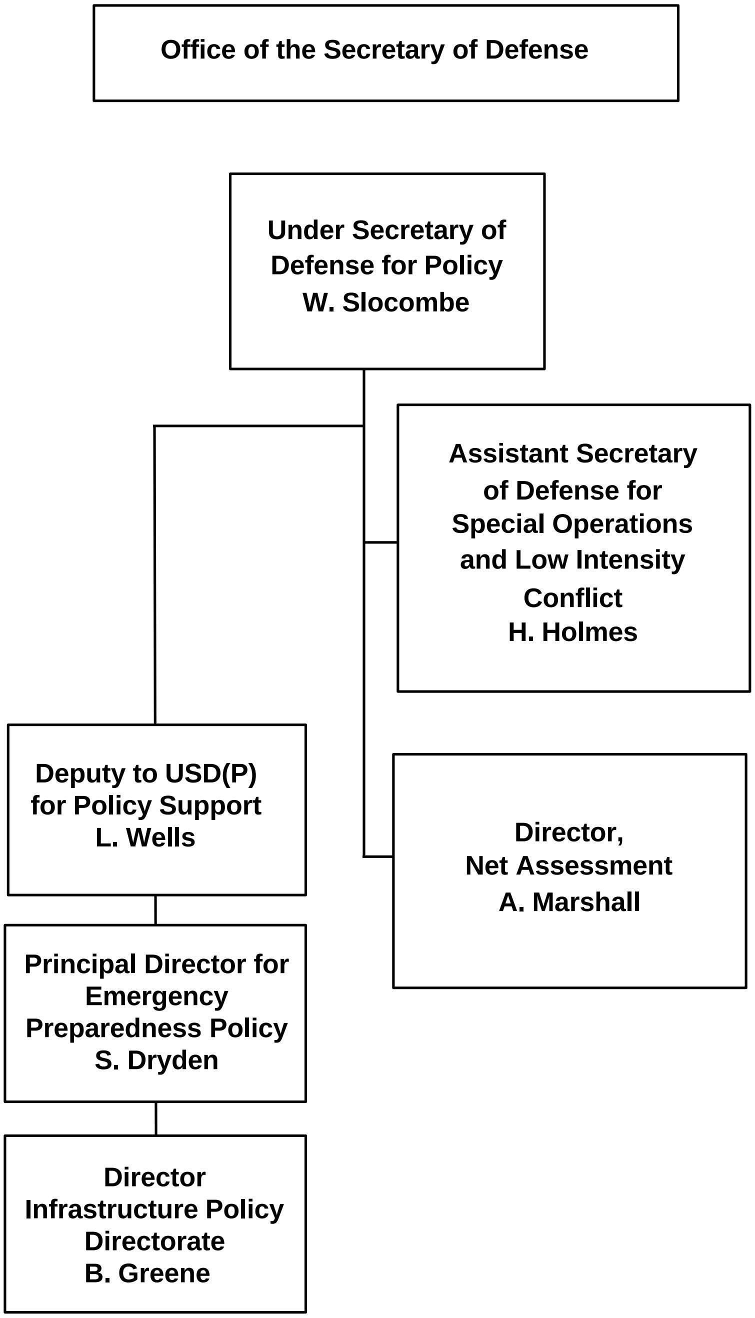
On-Line Resources:

Information Assurance Related Missions and Functions:

The Infrastructure Policy Directorate is responsible for shaping policy issues pertaining to DoD infrastructure and future directions for information protection, including interagency and interdepartmental coordination.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- Developed extensive "out-of-box" methodology for identifying dependencies within various infrastructures, critical nodes in the infrastructures, and dependencies among several infrastructures. Methodology includes modeling and simulation of industries and of the synergy between industries and infrastructures.
- Looking very closely at vulnerabilities of Supervisory Control and Data Acquisition (SCADA) networks.
- Need to add network and modeling and simulation expertise to our intelligence estimates.
- Concerned about how to insert infrastructure thinking into the Department of Defense processes - Defense Planning Guidance, Contingency Planning Guidance, National Military Strategy, National Security Strategy.
- Attempting to shape the role of DoD in the protection of infrastructures, including coordination between DoD and non-DoD government, and civilian/corporate owned/operated infrastructures.
- A National Defense Infrastructure Survivability Study was recently completed.
- The new-published Defense Planning Guidance directs the DoD components to investigate and assess their vulnerabilities and reliance on supporting infrastructures.


Office of the Secretary of Defense
Under Secretary of Defense for Policy W. Slocombe
Assistant Secretary of Defense for Special Operations and Low Intensity Conflict H. Holmes
Deputy to USD(P) for Policy Support L. Wells
Director, Net Assessment A. Marshall
Principal Director for Emergency Preparedness Policy S. Dryden
Director Infrastructure Policy Directorate B. Greene

Organization: Office of Net Assessments (OSD/NA)

Senior Information Warfare Official:

Director, OSD/NA, Andrew W. Marshall

Information Warfare Points of Contact:

COL Chuck Miller, USAF, Military Assistant
CAPT Jim FitzSimonds, USN, Military Assistant
CDR Jan van Tol, USN, Military Assistant
COL Scott Rowell, USA, Military Assistant

On-Line Resources:

Information Warfare Related Missions and Functions:

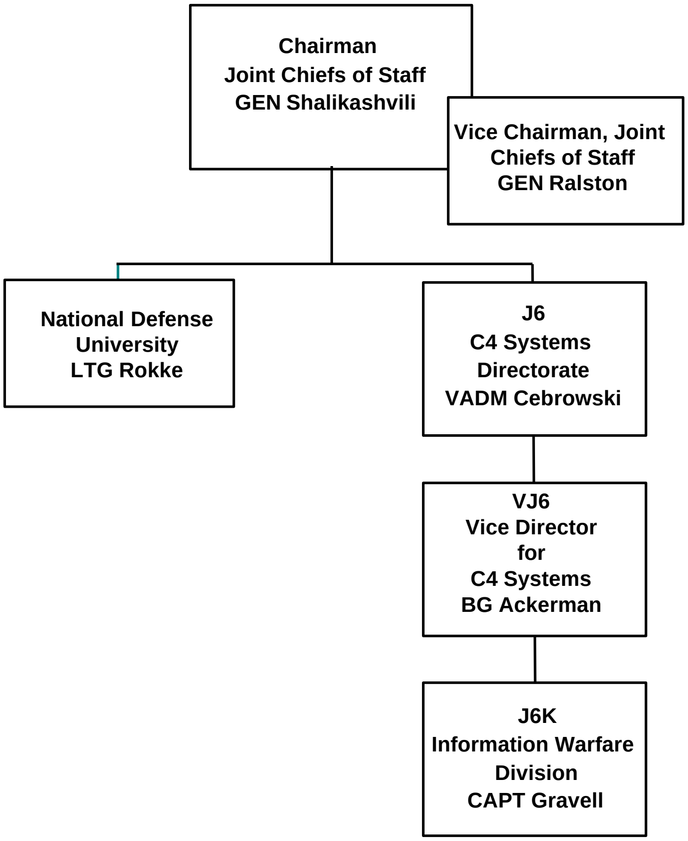
The Director of OSD/NA provides long-term analytic support to the Secretary of Defense and, when the SECDEF directs, to other senior officials in the Department (USD(P), USD (Acquisition), the Chairman, JCS, and the CINCs), on issues and trends in military affairs of potential import for the Department. Much of the analytic work of the office is engaged in preparing net assessments of the military balances in regions or in functional areas. The Director also makes recommendations regarding the DoD studies and analyses which are contracted outside the department. Information warfare was identified as a potentially important new warfare area several years ago in OSD/NA, and has been the subject of a widely ranging study effort ever since, within the office, and via contract, outside the office and with each of the Services and JCS.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- The Defense Science Board Summer (1994) Study on Information Architecture for the Battlefield recommended a Net Assessment to be done in the Department on IW. Their assessment was begun earlier this year. OSD/NA has set up advisory panels of key people from within the military and JCS to advise as this work is executed. Colonel Miller is currently the POC in OSD/NA for the Assessment.

- In addition to the Net Assessment, there is a long-term study effort under way which involves a series of workshops, seminars (IW Infrastructure, MOEs, Gaming and Simulation, Training, Intelligence, etc.), and wargames (Dec., 93, Oct., 94), as well as efforts with ASD/C3I and the Intelligence Community to explore the dimensions of IW, policy and strategy issues for the Department, and the policy issues relating to agencies beyond DoD of importance for the Department.

THE JOINT STAFF



Chairman
Joint Chiefs of Staff
GEN Shalikashvili

Vice Chairman, Joint
Chiefs of Staff
GEN Ralston

National Defense
University
LTG Rokke

J6
C4 Systems
Directorate
VADM Cebrowski

VJ6
Vice Director
for
C4 Systems
BG Ackerman

J6K
Information Warfare
Division
CAPT Gravell

Organization: The Joint Staff

Senior Information Warfare Official:

VADM Arthur K. Cebrowski, J6

Information Warfare Points of Contact:

CAPT William Gravell, Division Chief, Information Warfare Division, J6K
Major Steve Spano, Information Warfare Division, J6K

On-Line Resources:

Joint Staff Homepage: http://www.dtic.mil:80/defenselink/jcs/

Information Warfare Related Missions and Functions:

J6K is responsible for all national information assurance and defensive information warfare programs and activities coordinated by the Joint Staff.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- Ongoing training and education initiatives include implementing information warfare in exercises, coordinating Service training initiatives under the auspices of the Inter-Service Training Review Organization, and the conduct of an education strategy to infuse information warfare into the broad defense academic community by periodic visits to all engaged institutions.
- CJCSI 6510.01A, *Defensive Information Warfare Implementation*, has been produced and signed out. This builds upon broad policy in CJCSI 3210.01, *Information Warfare Policy*. Both were produced within the last year.
- The Joint Warfighter Capability Assessment (JWCA) process includes studies of information warfare offensive and defensive capabilities, emerging technologies, and intelligence support to IW. Additionally, the JWCA includes an effort to examine Service and Agency Program Objective Memorandum submissions relative to the Defense Planning Guidance and CINC requirements.
- J6K is studying nascent technologies outside of the requirements process to determine if some may have information warfare applications. The results of this study are provided in two documents:
  - Institute for Defense Analyses, *Information Warfare Technologies: Survey of Selected Civil Sector Activities*, IDA Document D-1792, February, 1996.
  - Institute for Defense Analyses, *Information Warfare: Selected Long-Range Technology Applications*, IDA Paper P-3157, February, 1996.
- J6K is leading an effort to develop rigorous modeling and simulation capabilities that would support CINC requirements for awareness of vulnerabilities of supporting national infrastructures. A Mission Needs Statement (MNS) for this capability is in final coordination.

- J6K is reexamining multi-level security (MLS) concepts and requirements and incorporating these concepts into information protection architecture efforts. J6K is working with the CINCs to define new MLS requirements and refine existing MLS requirements, and is establishing development and fielding priorities. These efforts are being validated by and within the JWCA process.
- The Joint Staff J6 recently completed an informative brochure entitled *Information Warfare, Implementing the Vision*. The brochure includes an IW-D implementation model which serves as an organizing construct for IW-D issues and activities.
- Preparation of Joint Doctrine for IW, Joint Pub 3-13, has been initiated. Joint Staff (J3) has the overall lead, with J6 responsible for defensive aspects and acting as technical review authority on the total effort.
- J6 is sponsoring a comprehensive examination of national IW-D issues by the Defense Science Board Task Force on Information Warfare Defense. The Task Force will report out in August 1996.

Organization: School of Information Warfare and Strategy (SIWS), Advanced Concepts, Technologies, and Information Strategies Directorate, Institute for National Strategic Studies, National Defense University (NDU)

Senior Information Warfare Official:

LTG Rokke, President, National Defense University
Dr. Hans Binnendjjk, Director, Institute for National Strategic Studies
Dr. David S. Alberts, Director, Advanced Concepts, Technologies, and Information Strategies
Dr. John Alger, Director, School of Information Warfare and Strategy (SIWS)

Information Warfare Points of Contact:

Col. (USMC, Retired) Bradley E. Barriteau, Professor, SIWS
Tom Czerwinski, Professor, SIWS
CDR Lee J. Ducharme, USN, Professor, SIWS
Lt. Col. Richard L. Casey, USAF, Executive Officer, SIWS
Dr. Fred Giessler, Professor, SIWS
Dr. Dan Kuehl, Professor, SIWS

On-Line Resources:

NDU Homepage: http:\\www.ndu.edu

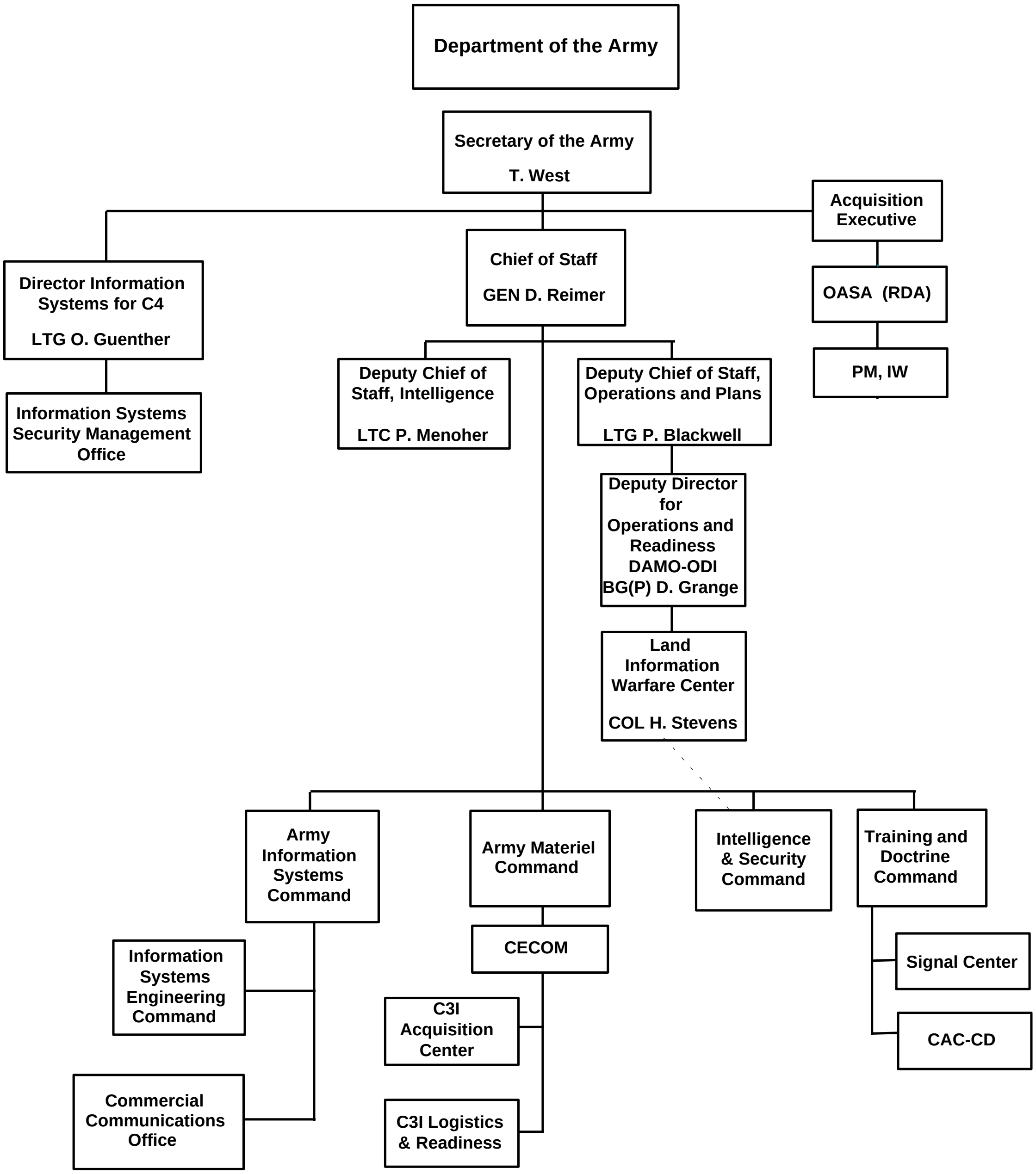
Information Warfare Related Missions and Functions:

The School of Information Warfare and Strategy graduated 32 students from its 10-month senior level (war college) program on 12 June 1996. The event marked the termination of the JCS-directed 2-year pilot as a stand alone senior-level program dedicated to the study of the information component of national power, but in recognition of the importance of information strategies, the President of the University has established a 3-tier program of information studies at the University. In the first tier, all colleges of the University will incorporate information studies into their curricula as appropriate to their respective missions. In the second tier, a slate of information strategies focused advanced studies will be offered to all senior-level students at the National Defense University, and in the third tier, an information strategies concentration program will be offered under the aegis of the School of Information Warfare and Strategy. The School of Information Warfare and Strategy will continue to offer its very popular 5-day Introduction to Information-Based Warfare Course for O-4, equivalents, and above and a 2-day executive course for O-6, equivalents, and above, which was first offered in April 1996. The School also offers a 2-day course in Chaos Theory for the Warrior.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- The combined force of the School of Information Warfare and Strategy and the Center for Advanced Concepts and Technology provides a center of excellence for the Department of Defense in the teaching and research of information warfare concepts. The combining of formerly separate research and teaching organizations results in the directorate of Advanced Concepts, Technologies, and Information Strategies. In addition to its teaching and research roles, this directorate is heavily engaged in outreach activities. It sponsors several conferences and workshops each year on topics germane to information warfare, and its members often speak on a variety of topics relevant to information warfare.

This page intentionally left blank.


Department of the Army
Secretary of the Army
T. West
Acquisition Executive
OASA (RDA)
PM, IW
Director Information Systems for C4
LTG O. Guenther
Information Systems Security Management Office
Chief of Staff
GEN D. Reimer
Deputy Chief of Staff, Intelligence
LTC P. Menoher
Deputy Chief of Staff, Operations and Plans
LTG P. Blackwell
Deputy Director for Operations and Readiness DAMO-ODI
BG(P) D. Grange
Land Information Warfare Center
COL H. Stevens
Army Information Systems Command
Information Systems Engineering Command
Commercial Communications Office
Army Materiel Command
CECOM
C3I Acquisition Center
C3I Logistics & Readiness
Intelligence & Security Command
Training and Doctrine Command
Signal Center
CAC-CD

Organization: Department of the Army

Senior Information Warfare Officials:

LTG Paul E. Blackwell, Deputy Chief of Staff, Operations and Plans
LTG Paul E. Menoher, Deputy Chief of Staff, Intelligence
LTG Otto J. Guenther, Director of Information Systems for C4 and Chief of Information

Information Warfare Points of Contact:

LTC Craig Jones, DAMO-ODI, ODCSOPS
Donal Harrison, DAMI-ST, ODCSINT
Phillip J. Loranger, Chief Command and Control Protect Division, Army Information Systems Security Management Office (ISMO), ODISC4

On-Line Resources:

Army Homepage: http://www.army.mil/default.htm
Army ODISC4: http://www.army.mil/disc4-pg/disc4.htm

Information Warfare Related Organizations, Missions and Functions:

Headquarters, Department of the Army formed a Command and Control Protect (C2 Protect) triad consisting of the Deputy Chief of Staff for Operations and Plans (DCSOPS), Deputy Chief of Staff for Intelligence (DCSINT), and the Director of Information Systems for Command, Control, Communications and Computers (DISC4) to “integrate C2 Protect into all facets of military operations.” [HQDA 1]

DCSOPS: DCSOPS has proponency for Information Warfare and addresses force modernization issues related to IW. Operational issues concerning IW are handled within the Directorate for Operations, Readiness, and Mobilization (DAMO-OD). The Directorate for Strategy, Plans, and Policy (DAMO-SSP) is responsible for coordinating IW policy in the Army while the Directorate for Force Development is responsible for coordinating and prioritizing IW requirements for the Army. DAMO-ODI is charged with operational management of the Army’s Command and Control Operations and has oversight of the Land Information Warfare Activity’s operations.

> Land Information Warfare Activity (LIWA): Established in March, 1995 at Fort Belvoir, Virginia, the LIWA, assigned to the U.S. Army Intelligence and Security Command, is under the operational control of DAMO-ODI, DCSOPS. An organizational summary for the LIWA follows.

DCSINT: In coordination with DCSOPS and DISC4, DCSINT is responsible for threat definition, establishment of policy and integrating counter-intelligence support to protect command, control, communications and computers.

DISC4: In coordination with DCSOPS and DCSINT, DISC4 is responsible for implementing procedural and material protective measures, to protect command, control, communications and computers and for the development, sustainment and management of the C2 Protect Library.

> Information Systems Security Management Office (ISMO) is subordinate to ODISC4. The mission of ISMO is to implement protective measures, both procedural and material, to protect Army command and control and implement lead responsibilities for the development, sustainment and management of the C2 Protect Plans.

Training and Doctrine Command (TRADOC) has established a Space and C2W Directorate to oversee IW related actions.

Information Warfare is integrated across the Army and implemented in the Force XXI initiative, therefore all Major Commands (MACOM) and other Army organizations are involved in planning, developing and implementing C2 Protect measures in the Army.

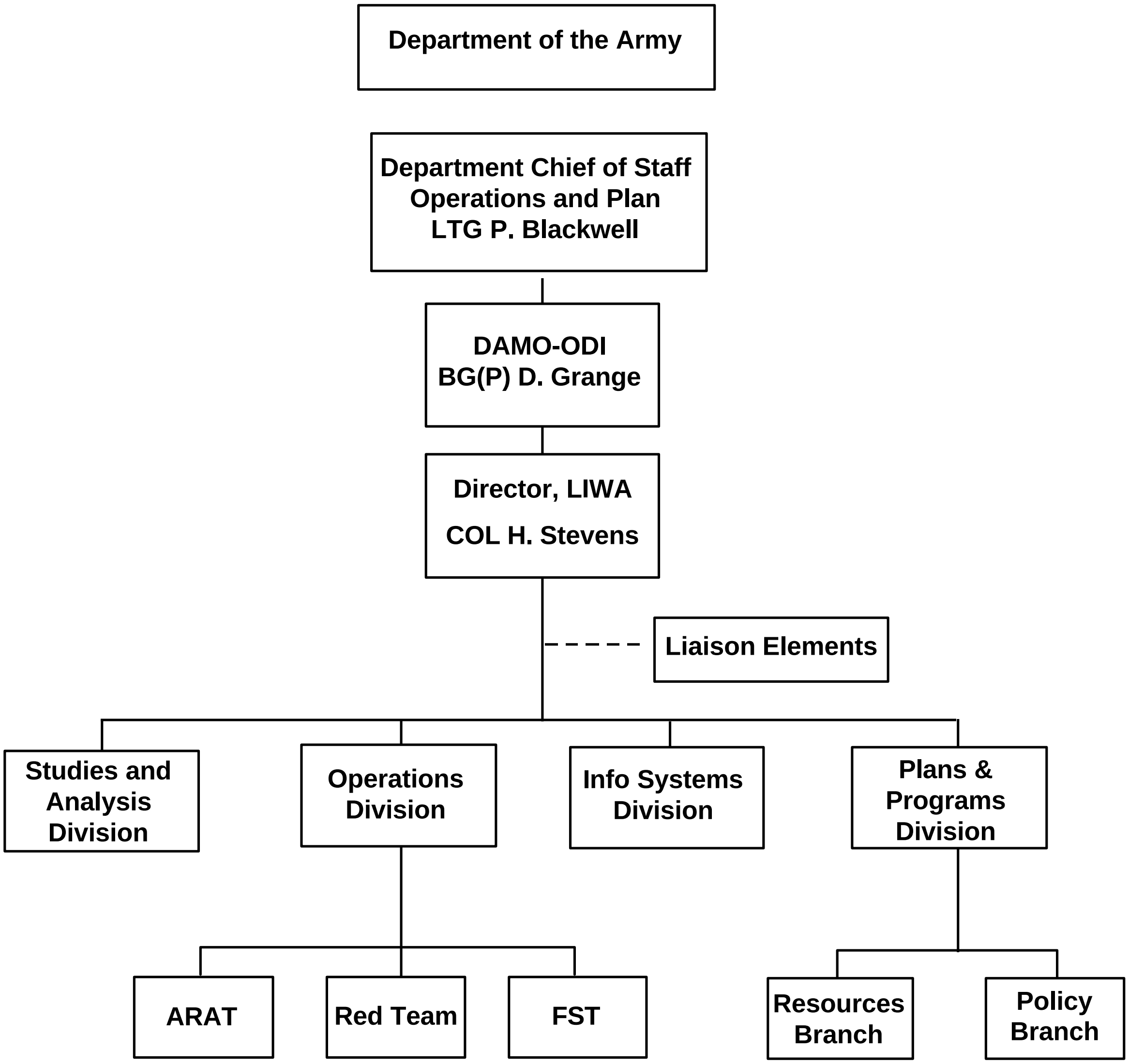
Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- The Army has adopted Information Operations (IO) doctrine and is integrating IO into Army doctrine, individual and unit training, leader development, force design, and material acquisition initiatives. TRADOC has published Field Manual 100-6, *Information Operations*, 15 April, 1996 [HQDA 2] The Army has adopted Information Operations for two reasons: to recognize that information issues permeate the full range of military operations (beyond the traditional context of war), from peace through global war; and to emphasize the tactical and operational aspects of information based warfare. Information Operations integrate all aspects of information to support and enhance the elements of combat power, with the goal of dominating the battle space at the right time, at the right place, and with the right weapons or resources. The Army supports or implements Information Warfare through Command and Control Warfare (C2W) actions." [HQDA 2] The components of IO are military information systems, intelligence, and command and control warfare. The IW-D component of IO is C2-Protect. The Army has adopted a risk management approach and stresses risk management over risk avoidance.
- The Army is using several steering groups and working groups as to help execute, and integrate information warfare across the Service and to provide executive oversight of the program. The IW General Officer Steering Group is chaired by the DAMO-OD, DCSOPS and includes representatives charged with implementing IW. The C2 Protect General Officer Steering Group is co-chaired by the DCSINT and the DISC4 and includes general officers from DCSOPS and the signal and acquisition communities. Established in late 1993, a C2 Protect Council of Colonels was formed to deal with the increasing burden of protecting the wide range of C2 assets essential to the success of IW. The Council, chaired by ISMO, meets quarterly and addresses current Army C2 Protect issues.
- In January 1995, the DISC4 established an Army C2 Protect Working Group and tasked it to develop the C2 Protect Library. Membership includes a broad range of Army organizations. The C2 Protect Library consists of six volumes:

VOL 1 C2 Protect Program Management Plan, August 1995
VOL 2 C2 Protect Master Training Management Plan, 18 January 1996
VOL 3 C2 Protect Implementation Plan, 29 February 1996
VOL 4 Intelligence Support C2 Protect Action Plan, Draft
VOL 5 C2 Protect Resourcing Proposal, May 1996, Draft
VOL 6 A C2 Protect Automation Threats Overview, SECRET, 14 February 1996.

Volumes 1, 2, 3, 6 have been published. Volumes 4 and 5 are in draft. In addition to the C2 Protect Library, key Army regulations for information security (AR 380-19), intelligence requirements (AR 381-11), and acquisition (AR 25 and 70) have been revised to incorporate C2 Protect. Additionally, the Army is issuing policy messages directing C2 Protect tactics, techniques, and procedures.

- Protect: The Army is leveraging the efforts of DISA and the other Services to provide system administrators with the capability to scan and monitor systems, to audit systems and reduce audit data, to identify and patch system vulnerabilities, to eradicate viruses, and to implement password protection programs. It has identified and issued two automated sets of tool boxes for use by Automated Information System Mangers to help them protect their information environments. Also, the Army co-chairs, with DISA, the OSD Common Tools Working Group and advises the Army organizations of tools available from DISA and of the services provided by the DISA ASSIST Help Desk.
- Training, Education and Awareness: In addition to the training necessary for the unique technical skills required for LIWA operations, the Army has established training for system administrators and information system security managers. Awareness training is provided for users and includes executive level training.
- Acquisition: Increased emphasis is being placed on embedding security into development programs. Efforts include revised acquisition regulations with stiffer security requirements, monitoring of Major Automated Information System Review Council (MAISRC) programs, and closer attention paid to requests for security waivers. The Department of the Army Technical Architecture (ATA), published on 30 January 1996, applies to all systems that produce, use, or exchange information electronically and includes information security standards. The ATA was used as a model for the recently published draft Joint Technical Architecture. The Army Enterprise Strategy, the Army Modernization Plan, and the ATA provide broad, high level information warfare and C2 Protect guidance for program developers.
- Resourcing: The C2 Protect Resourcing Proposal (VOL 5 of the C2 Protect Library) is in Final Draft. This volume, in concert with the other volumes of the Plan, defines the c2 Protect program resourcing instructions and justification for resourcing all twelve C2 Protect initiatives. In the short term, implementation of the C2 Protect program has outpaced resources.


Department of the Army
Department Chief of Staff Operations and Plan LTG P. Blackwell
DAMO-ODI BG(P) D. Grange
Director, LIWA
COL H. Stevens
Liaison Elements
Studies and Analysis Division
Operations Division
Info Systems Division
Plans & Programs Division
ARAT
Red Team
FST
Resources Branch
Policy Branch

Organization: Land Information Warfare Activity (LIWA)

Senior Information Warfare Official:

COL Halbert Stevens, Commander, LIWA

Information Warfare Points of Contact:

LTC Tom Hudson, Deputy Commander, LIWA

On-Line Resources:

Information Warfare Related Organizations, Missions and Functions:

Established in March, 1995 at Fort Belvoir, Virginia, the LIWA, assigned to U.S. Army Intelligence and Security Command, is under the operational control of DCSOPS. The mission of the LIWA is to provide Department of the Army level Information Warfare/Command and Control Warfare support to Land Components and separate Army commands to facilitate planning and execution of information operations. The LIWA coordinates with National, Joint, and Service IW/C2W centers to exchange and synchronize intelligence and information support across the operational continuum. The LIWA provides supports teams to facilitate operational planning and is responsible for conducting Army vulnerability assessments, providing computer emergency response, and Red Teaming.

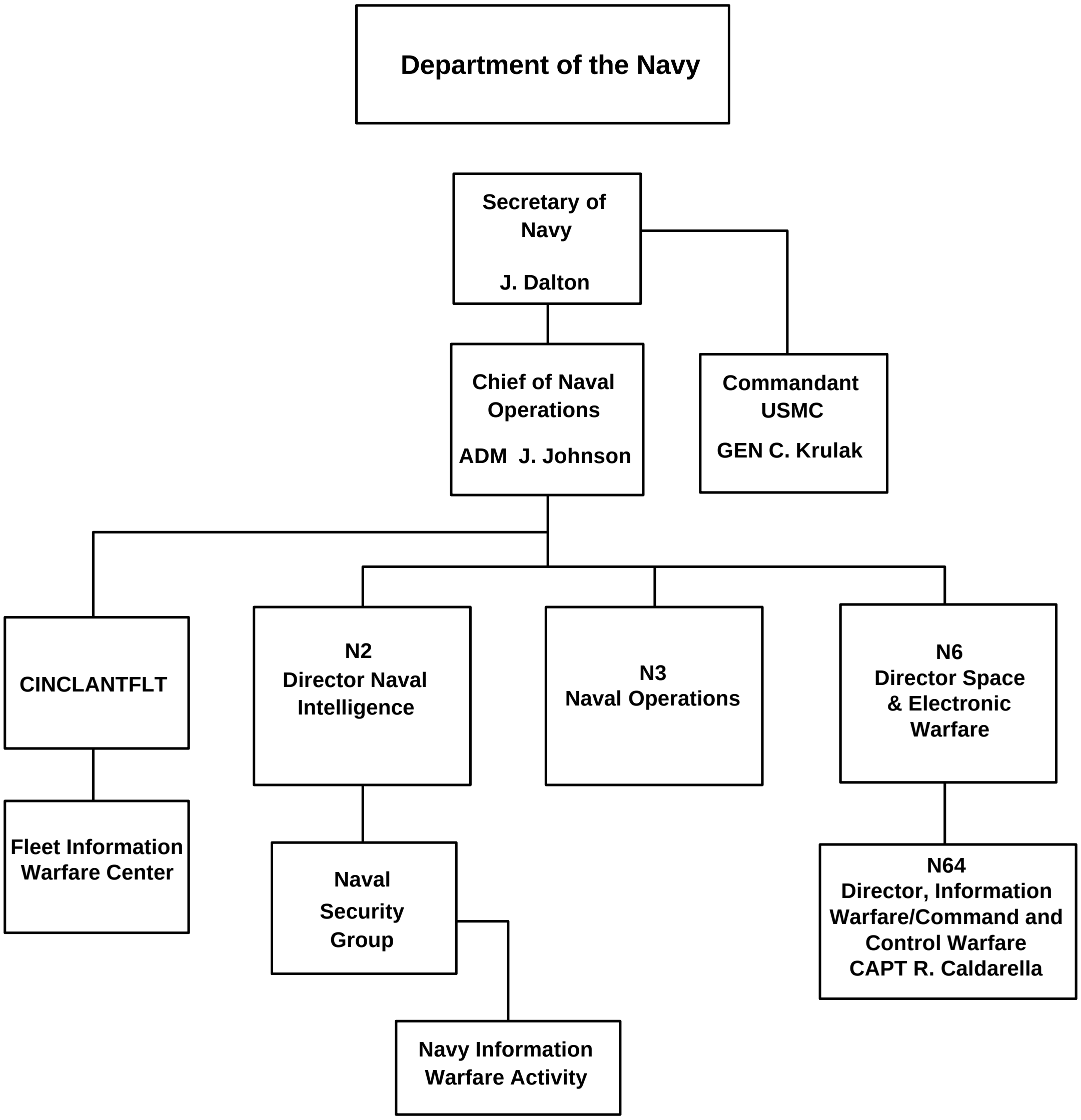
Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- The Army is in the process of incorporating LIWA capabilities into day-to-day operations. LIWA capabilities are addressed in the FM 100-6 [HQDA 2] and an official Table of Distribution and Allowance; to refine LIWA staffing, is being developed.
- A key mission of the LIWA is to provide computer emergency response support to Army forces. To meet the increasing demand for computer emergency response, the Joint Requirements Oversight Council (JROC) recommended that the Army develop an organic computer emergency response capability similar to the capabilities of the other Services. The LIWA is building the Army central emergency response capability and will soon become a member of the Forum of Incident Response and Security Teams (FIRST). LIWA is also building the Continuity of Operations (COOP) site for the DISA ASSIST.

The Army is implementing a centralized react and reporting capability. This includes finalizing an MOU with DISA with respect to incident reporting and collocating and integrating computer security skills with the four Army Regional Network Management Centers. Augmenting these with counterintelligence, law enforcement, and legal assets is under consideration. The first Regional CERT was established in USAREUR on 1 February, 1996. It currently supports the European Theater to include Operation Joint Endeavor and uses an Automated Intrusion Monitoring System (AIMS) tool to monitor theater hosts.

- VAAP: The Army has adopted the DISA Vulnerability Assessment and Analysis Program (VAAP). Findings and fixes are promulgated by the Army staff and incorporated into tactics, techniques and procedures. DISA provides VAAP support for the sustaining base and LIWA for the tactical environment.
- Red Teaming: LIWA is building a capability to provide Red Teaming support for the Army in the field. The Army Digitization Office (ADO) has the lead for TF XXI. ADO uses LIWA assets for TF XXI Red Teams.

This page intentionally left blank.


Department of the Navy
Secretary of Navy
J. Dalton
Chief of Naval Operations
ADM J. Johnson
Commandant USMC
GEN C. Krulak
CINCLANTFLT
N2
Director Naval Intelligence
N3
Naval Operations
N6
Director Space & Electronic Warfare
Fleet Information Warfare Center
Naval Security Group
N64
Director, Information Warfare/Command and Control Warfare
CAPT R. Caldarella
Navy Information Warfare Activity

Organization: Department of the Navy

Senior Information Warfare Officials:

VADM J. P. Reason, Deputy Chief of Naval Operations for Plans, Policy and Operations (N3/N5)
VADM W. J. Davis, Jr., Director, Space, Command and Control, and Information Warfare (N6)
RADM T. F. Stevens, Commander, Naval Security Group Command/EA for IW

Information Warfare Points of Contact:

CAPT R. J. Caldarella, Director, Information Warfare/Command and Control Warfare Division (N64), Office of the Chief of Naval Operations
CAPT M. V. Sherrard, Deputy Director, Information Warfare/Command and Control Warfare Division (N64B), Office of the Chief of Naval Operations
E. Owen, Defensive Information Warfare Branch (N643), Information Warfare/Command and Control Warfare Division, Office of the Chief of Naval Operations
CDR J. Stratton, Staff Ops & Plans, Special Warfare Objective (OPNAV N513)
CDR E. Kanerva, Assistant Chief of Staff for IW/C2W, CNSG (CNSG N6)

On-Line Resources:

Navy Homepage: http://www.navy.mil
FIWC NAVCIRT Homepage: http://www.fiwc.navy.mil
NRL Homepage: http://www.cmf.nrl.navy.mil

Information Warfare Related Organizations, Missions and Functions:

The Deputy Chief of Naval Operations for Plans, Policy and Operations (N3/N5) is responsible for developing Navy IW/C2W policy, strategy and operational concepts including operations security (OPSEC).

The Director, Space, Command and Control, and Information Warfare (N6) is responsible for overall IW/C2W development and implementation guidance to include establishment of IW/C2W objectives and procedures. The Information Warfare/Command and Control Warfare Division (N64) is responsible for the development of requirements, plans, and IW programs in the Navy. The office is the day-to-day point of contact for all IW matters in the Navy. Inside N64, the Defensive Information Warfare Branch (N643) serves as sponsor of the Navy INFOSEC Program including program development, implementation, planning, and budgeting.

The Commander, Naval Security Group, serves as CNO's (N6) Executive Agent (EA) for Navy IW, overseeing all manpower, training, and equipment requirements that are associated with IW. The IW EA, in coordination with CNO N6/N8, the Navy Systems Commands, and other appropriate agencies, reviews and documents requirements for development, procurement, training, deployment, and life cycle support of Navy IW systems. Additionally, the IW EA, in conjunction with the Chief of Naval Education and Training, Naval Doctrine Command, and the Fleet Information Warfare Center (FIWC), is responsible for ensuring IW doctrine and concepts, including IW protect, is included in appropriate Navy training programs for Navy personnel throughout their careers.

The Space and Naval Warfare Systems Command has established a program directorate (PD-16) for Information Warfare. PD-16's mission is to develop, procure, field, and support interoperable Navy IW systems. PD-16 additionally serves as the Navy INFOSEC execution agent for DoN and DoD/National agencies. A primary function of PD-16 is to serve as the Navy's single point of entry into the IW acquisition community. PD-16 is supported by three program managers who manage the development, acquisition, integration, and life cycle support of programs for navy IW systems. IW protect systems are managed by PMW 161, the Information Systems Security (INFOSEC) Program Office. PMW 161 is the designated point of contact for DoN interface with NSA for all key management, embedded crypto, and other INFOSEC matters.

The Office of Naval Intelligence (ONI) is the focal point for intelligence and threat support to Navy-related IW/C2W programs and coordinates with the intelligence community for satisfaction of Navy IW/C2W requirements. ONI will also develop all source intelligence indicators that will contribute to establishing Measures of Effectiveness for Navy IW/C2W tactics and weapons.

The Fleet Information Warfare Center (FIWC), established 1 Oct 1995, is the Navy's IW Center of Excellence, and is the principle agent for development of IW/C2W tactics, procedures, and training. FIWC deploys personnel trained in IW protect disciplines and equipped with appropriate hardware, including C-2 protect hardware and software systems, to support battle group and joint task force operations. Additionally, FIWC provides Navy Computer Incident Response Teams (NAVCIRT), and acts as the Navy's single point of contact for information systems monitoring, leveraging capabilities found in the reserves and NSGA Pensacola.

The Naval Information Warfare Activity (NIWA), acts as CNO's technical agent for the pursuit of information warfare related technologies. As such, NIWA conducts technical threat analysis and vulnerabilities assessment studies, develops technical requirements for, and evaluates/assesses new information technologies, competitive architectures, and advanced concepts for Navy defensive IW systems.

The Director, Communications Security Material System, a third echelon command under COMNAVCOMTELCOM, acts as the Central Office of Record for DoN assurance hardware and software.

Reflecting the cross-cutting nature of IW/C2W, implementing instructions assign responsibilities across the full spectrum of Navy command and staff activities. The organizations and functions described above reflect key Navy organizations responsible for implementing and institutionalizing IW/C2W in the Navy. In addition to these, the Fleet CINCs, Numbered Fleet Commanders, and Battle Group Commanders have IW/C2W Commanders and a supporting staff assigned. A portion of this staff is dedicated to IW defensive issues, including the protection and assurance of information systems and the data contained therein.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- The Navy subscribes to the direction provided in DoD Instruction TS3600.1 and CJCS MOP 30. The Chief of Naval Operations (CNO) IW-D strategy includes investment in protective technologies; reform of the acquisition process, operational integration of the security disciplines, and use of a risk management process rather than a risk avoidance. An update of the Navy (DoN) policy OPNAVINST 5239.xx will require that all information services (voice, video, imagery, data) be protected; that all unclassified systems be considered sensitive; and requires all sensitive systems to implement network security management tools to monitor, detect, isolate, and react. DoN policy also requires all classified systems, in addition to encryption, to implement identification/ authentication and network security management tools. Two key documents issued by the CNO are OPNAVINST 3430.25, Information Warfare and Command and Control Warfare, April 1994, which established Navy IW policy and assigned responsibilities, and OPNAVINST 3430.26, Implementing Instruction for Information Warfare/Command and Control Warfare (IW/C2W), 17 January 1995 which issues implementing guidance and organizational relationships. Overall doctrine for IW/C2W is found in Navy Doctrine Publication (NDP) 3, *Naval Operations.* The Fleet Information Warfare Center (FIWC), in conjunction with the Naval Doctrine Command, is developing specific IW/C2W doctrine to be promulgated in the following publications:

    - Naval Warfare Pub 3-13 (Naval IW)
    - Naval Warfare Pub 3-13.1 (Naval C2)
    - Naval Warfare Pub 3-14.1.1 (Navy C2W/C2W Commander's Manual).

- Panels and Working Groups: The Navy has established a Navy Information Warfare Council to foster closer working relationships between Navy organizations responsible for Navy IW program planning and execution, and to institutionalize IW throughout the Navy. The council is comprised of the senior 0-6 from each of the key Navy commands supporting IW. Additionally, specific Navy organizations have established internal working groups to help implement IW/C2W. The N3/N5 has established a Strategic Planning Cell to develop and coordinate OPNAV IW/C2W strategy and policy. The INFOSEC Engineering Working Group (IEWG), chaired by SPARWAR PMW-161, consists of senior engineers from system command, laboratories, and contractors and establishes technical strategies for the Information Assurance/INFOSEC Program. Additionally, OPNAV N643 chairs a Vulnerability Assessment, Countermeasures Tools Working Group that will consolidate and focus Navy resources to upgrade and expand assessment and monitoring capabilities.

- Protect and Detect: The Naval Research Laboratory (NRL) took the publicly available S/Key™ onetime password system developed by Bellcore, added a stronger algorithm, then released the code back to the Internet. A variety of Navy and other DoD sites are using the NRL enhanced system to provide much stronger hacker protection for hosts and firewalls. The Navy is pursuing crypto options for Shipboard Secure Phone and participating in the Digital Voice Processor Consortium. A priority long term effort is to enhance the security protocols that will be used on the Fleet Internet. NRL will develop and implement standardized security mechanisms for the next generation of the Internet that will make COTS products available to the Navy and DoD with the appropriate security attributes. NRL security protocols are included in the Internet Protocol, version 6 (IPv6) proposal. The security mechanisms are algorithm-independent and support both commercial and military needs. The Navy/USMC has identified funds within their POM which sufficiently cover firewalls and guards as required to protect their connections to DISN. They have also funded for their internal needs. The Navy is modifying the Ice Pick™ tool with NRL technology to allow a central administrator to probe a PC network for vulnerabilities.

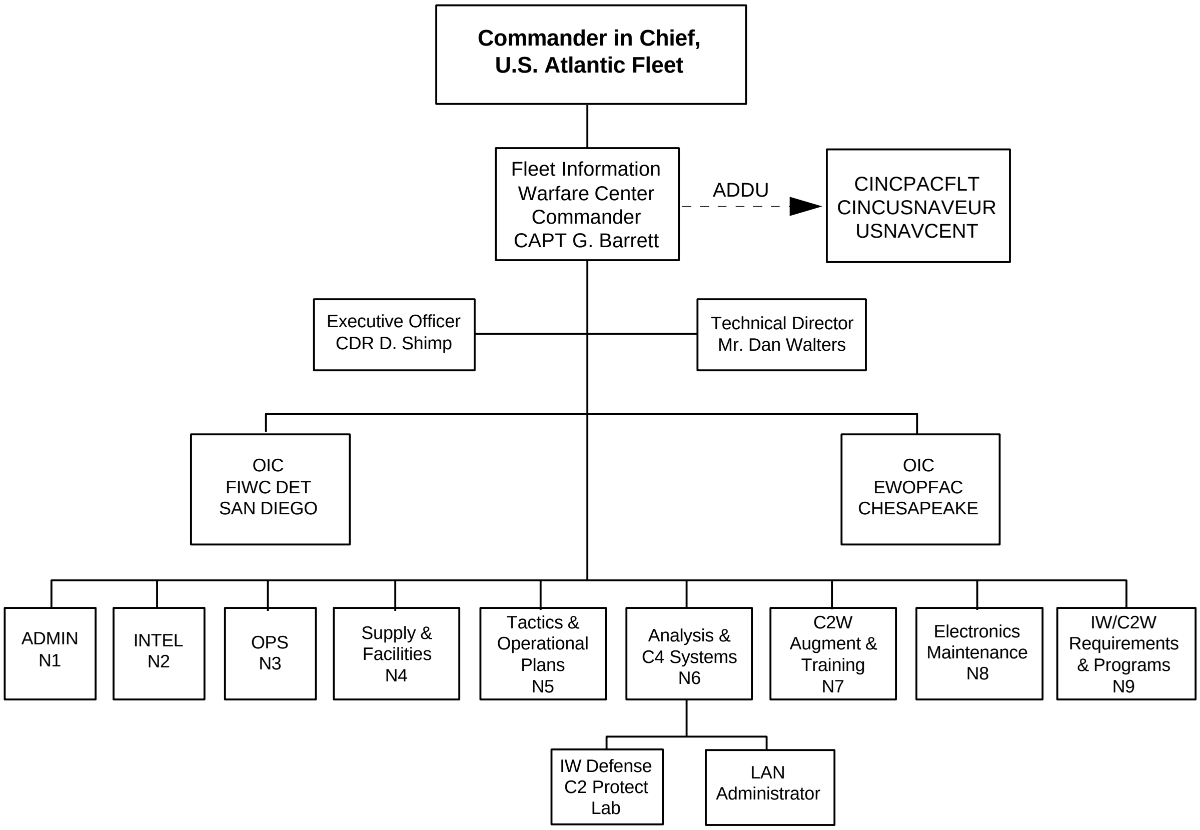
- Training, Education and Awareness: The Chief, Naval Education and Training (CNET) (N7) is designated as lead for IW training, formally referred to as DoD Interservice Training Review Organization (ITRO) Initiative for Joint IW Training (DITJIT) as of May 1995. The following training programs have been developed and/or have been initiated:

  - Awareness Training - Basic to Master level program consisting of:
    - Basic Officer and Enlisted "A" School "Introduction to IW/C2W"
    - Department Head/Journeyman Level Schools "Fundamentals of IW/C2W"
    - CO/XO and Enlisted Master Level School "IW/C2W Advanced Application"
    - Specialized Modules Training - A four element program consisting of
      - ◊ IW/C2W for Intel Pros
      - ◊ IW/C2W for USN/USAF EWOs
      - ◊ IW/C2W Common Core CBT
      - ◊ Formal Schools - "Retooled"

        -- "Network Security & Vulnerability Technician"
        -- "Nodal Analysis Technician"
        -- DoD-Common COI for System/Network
    - Administrators

- Acquisition: The Navy will direct the incorporation of security standards in Navy programs via a proposed SECNAV Instruction 5200.1-M, Naval Program Protection Plans. Non-centrally purchased AIS will be required to incorporate standard INFOSEC products and procedures. In addition, the Navy will establish a realistic vulnerability assessment/certification and accreditation process.

This page intentionally left blank.


Commander in Chief,
U.S. Atlantic Fleet
Fleet Information Warfare Center Commander CAPT G. Barrett
ADDU
CINCPACFLT
CINCUSNAVEUR
USNAVCENT
Executive Officer CDR D. Shimp
Technical Director Mr. Dan Walters
OIC FIWC DET SAN DIEGO
OIC EWOPFAC CHESAPEAKE
ADMIN N1
INTEL N2
OPS N3
Supply & Facilities N4
Tactics & Operational Plans N5
Analysis & C4 Systems N6
C2W Augment & Training N7
Electronics Maintenance N8
IW/C2W Requirements & Programs N9
IW Defense C2 Protect Lab
LAN Administrator

Organization: Fleet Information Warfare Center

Senior Information Warfare Official:

CAPT G. A. Barrett, Commanding Officer

Information Warfare Points of Contact:

Dan Walters, Technical Director
Bill Jones, Analysis and C4 Systems Department Head
LCDR Dean Rich, C2 Protect Division Officer

On-Line Resources:

FIWC NAVCIRT Homepage: http://www.fiwc.navy.mil

Information Warfare Related Organizations, Missions and Functions:

The FIWC is the Navy's IW Center of Excellence. The FIWC is located at Little Creek Amphibious Base, VA with a detachment in San Diego, CA. FIWC missions include:

- Act as the Fleet CINC's principal agent for development of IW/C2W tactics, procedures, and training, under the operational control of Commander in Chief, U.S. Atlantic Fleet (CINCLANTFLT), additional duty to Commander in Chief, U.S. Pacific Fleet (CINCPACFLT), Commander in Chief, U.S. Naval Force Europe (CINCUSNAVEUR), and Commander, U.S. Naval Forces Central Command (CMUSNAVCENT). Deploy personnel trained in the IW/C2W disciplines of exploit, protect, and attach with appropriate counter-C2/C-2 protect hardware and software systems to support Battle Group and Joint Task Force operations.
- In coordination with the Fleet CINCs, Numbered Fleet Commander, and COMNAVDOCCOM, develop and disseminate integrated naval IW/C2W tactics, techniques, and procedures to Fleet units and shore support establishments worldwide.
- Coordinate naval IW/C2W tactics, procedures, and training with the joint centers and the other services' IW/C2W related centers.
- Maintain liaison with national agencies, other service centers, and the Naval Information Warfare Activity (NAVINFOWARACT) to facilitate satisfaction of IW/C2W related requirements submitted by the Fleet.
- Provide to the CNO, Fleet CINCs, COMNAVSECGRU, and NAVSYSCOMs advice, assistance, and recommendations on requirements and priorities for research and development, procurement, and training which supports IW/C2W applications.
- Provide IW/C2W protect teams to support operational and shore establishments.
- An Information Manager security officer will augment and deploy as part of each Battle Group's IW Commander's staff.

FIWC provides Navy operating forces and shore establishments with the following support:

- Deployable shipboard IW teams
- Offensive and defensive IW support
- Signals intelligence exploitation
- On-line computer surveys (Vulnerabilities)
- Computer Incident Response Team (Emergency Response)
- Train and equipment Battle Group Staffs (Training)

To support Defensive IW, FIWC provides the following services to support DoN information systems:

- Navy Computer Incident Response Team (NAVCIRT). Provides computer security and incident response capabilities for fleet and shore-base commands. Serves as the Navy's clearinghouse for knowledge and tools related to IW/C2W Protect.
- Vulnerability Analysis and Assessment Program. Provides DoN commands with an analysis of their computer networks to identify vulnerabilities. The VAAP operates SUN SPARC workstations, with the capability to conduct unclassified to Top Secret level assessments.
- Automated Security Incident Measurement (ASIM). Navy has initiated the use of ASIM on Battle Groups classified systems. The ASIM provides improved monitoring capability for the information system operator, and is laying the groundwork for a Navy-wide initiative to integrate monitoring, detection, isolation, and reaction capabilities into security architectures. ASIM recognizes attempts by unauthorized personnel to gain access to Navy networks, notifies appropriate personnel of the intrusion attempt, and automatically records the intrusion.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- The FIWC hosts the IW/C2W lessons learned database.
- Results of On-Line Surveys have raised awareness at senior level regarding vulnerabilities to sensitive but unclassified systems, and classified systems built on COTS products.
- Navy has built strong working relationships with other Services and DISA CERT organizations, and has gone to great extent to share lessons learned and tools.
- Navy has conducted numerous follow-on assessments on behalf of organizations to determine improvements to systems security. These assessments have been integral to increased system administrator training and awareness.

Organization: Naval Information Warfare Activity

Senior Information Warfare Official:

CAPT T. Daly, Commanding Officer

Information Warfare Points of Contact:

LCDR R. Zellman

On-Line Resources:

Information Warfare Related Organizations, Missions and Functions:

The Naval Information Warfare Activity (NIWA) is headquartered at Fort Meade, MD, with subordinate organizations at the Naval Research Laboratory, Washington, DC, and the National Maritime Intelligence Center, Suitland, MD. The NIWA is the CNO's principal technical agent and interface to Navy and national Agencies pursuing information warfare technologies. In this role the NIWA acts as technical agent for development and acquisition of navy special technical capabilities supporting IW systems.

The NIWA also serves as the Navy's technical agent for appropriate simulation and modeling activities supporting IW.

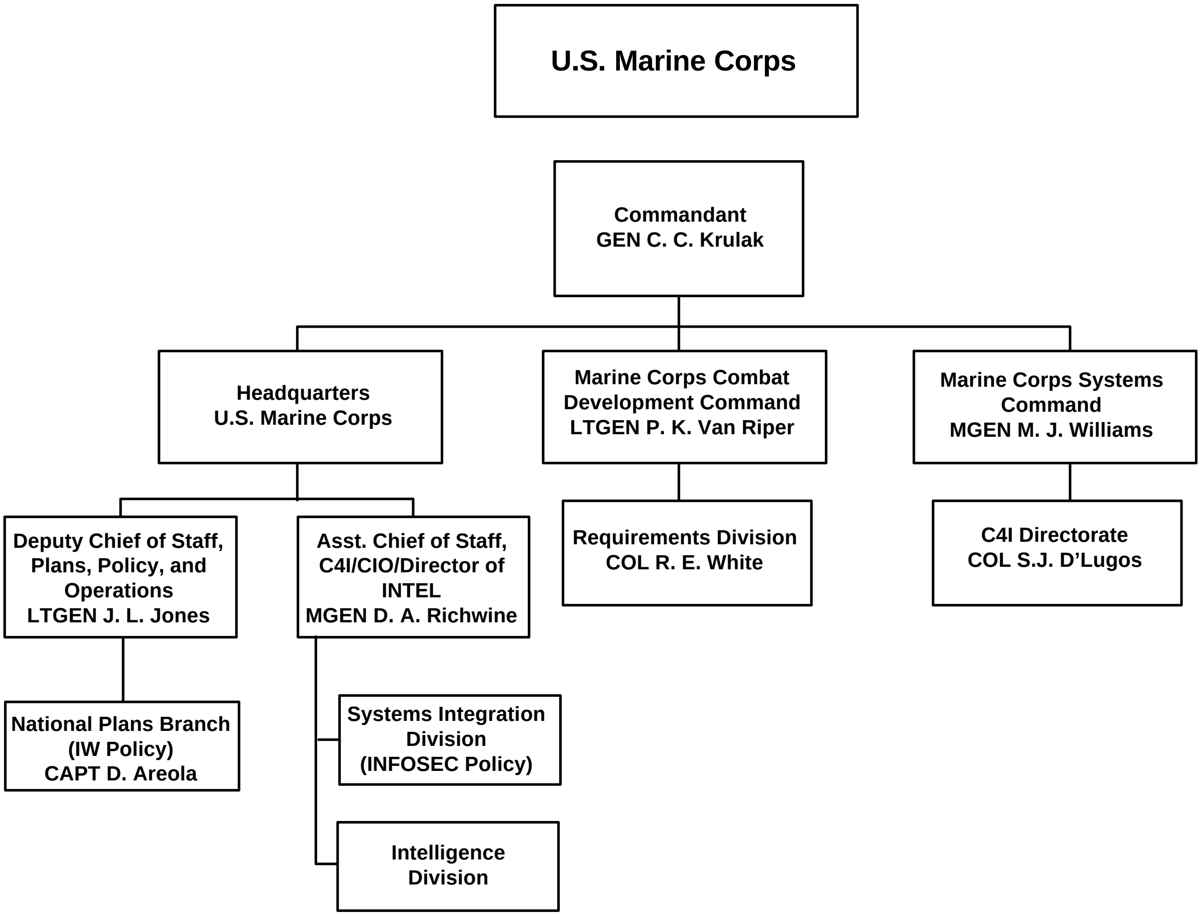
NIWA mission is to:

- Act as CNO's principal technical agent and interface to Service and national level agencies engaged in the pursuit of information warfare technologies.
- Conduct technical liaison with appropriate national agencies and provide resulting information warfare data/data bases to CNO (N6), COMNAVSECGRU, and the FIWC, et al.
- Conduct and/or manage all technical partnership activities with national-level agencies for technology development and IW applications and provide relevant IW data to CNO (N6), COMNAVSECGRU, FIWC, to support IW/C2W operations planning.
- Act as the principal technical interface with FIWC for transition of IW special technical capabilities for naval and Navy-supported joint operations.
- In accordance with current tasking, act as technical agent for development and acquisition of Navy special technical capabilities supporting IW systems.
- Conduct technical threat analysis and vulnerabilities assessment studies, develop technical requirements for, and evaluate/assess new information technologies, competitive architectures, and advanced concepts for offensive and defensive IW systems.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- A key role of NIWA is to perform RF vulnerability assessments for developing Navy systems, i.e., satellite systems such as MILSAT, and INMARSAT. As IW initiatives have focused on networks and interconnectivity, NIWA is focusing on efforts to assess a "system of systems."
- NIWA is developing a better mechanism to identify information systems vulnerabilities in the conceptual or design phase. Further, NIWA is attempting to prioritize which critical systems demand vulnerability assessments.
- To increase the usefulness of vulnerability assessments, NIWA is developing a standard vulnerability assessment report that will be more meaningful to the acquisition community.
- The results of vulnerability assessments will be combined with more precise threat assessments, recommended countermeasures, and minimum risk guidance enabling the Program Manager to make objective risk management decision.

This page intentionally left blank.


U.S. Marine Corps
Commandant
GEN C. C. Krulak
Headquarters
U.S. Marine Corps
Marine Corps Combat Development Command
LTGEN P. K. Van Riper
Marine Corps Systems Command
MGEN M. J. Williams
Deputy Chief of Staff, Plans, Policy, and Operations
LTGEN J. L. Jones
Asst. Chief of Staff, C4I/CIO/Director of INTEL
MGEN D. A. Richwine
Requirements Division
COL R. E. White
C4I Directorate
COL S.J. D'Lugos
National Plans Branch
(IW Policy)
CAPT D. Areola
Systems Integration Division
(INFOSEC Policy)
Intelligence Division

Organization: United States Marine Corps

Senior Information Warfare Officials:

LtGen A. C. Blades, Deputy Chief of Staff for Policy, Plans, and Operations
MajGen D. Richwine, Assistant Chief of Staff for C4I/Director of Intelligence

Information Warfare Points of Contact:

Capt Dave Areola, National Plans Branch, ODCS for Policy, Plans, and Operations
Major Bob Wiedower, National Plans Branch, ODCS for Policy, Plans, and Operations
LtCol Marshall Snyder, Systems Integration Division, ACS, C4I

On-Line Resources:

U.S.M.C. Homepage: www.usmc.mil

Information Warfare Related Organizations, Missions and Functions:

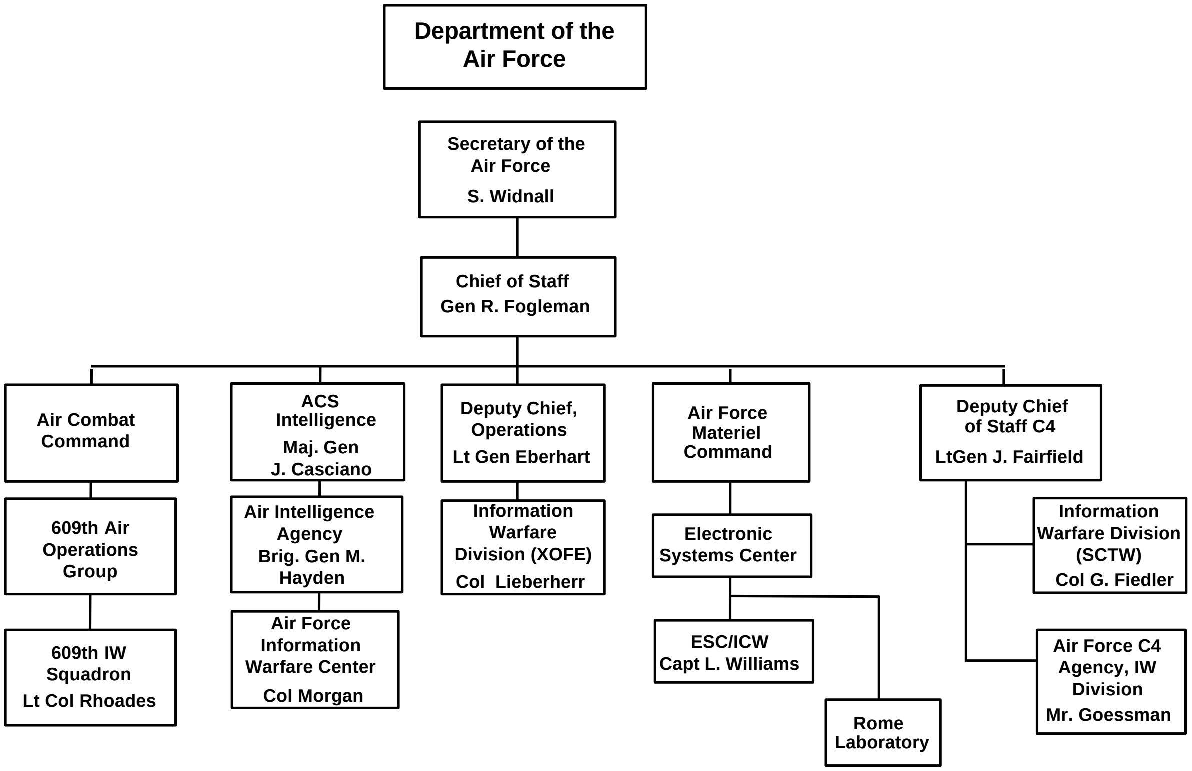
Headquarters, Marine Corps (HQMC) is responsible for IW-D policy. The National Plans Branch within the Plans, Policy and Operations Department, HQMC is responsible for IW and C2W policy. The C4I Department, HQMC is charged with INFOSEC and COMPUSEC policy. Combat Developments Command is responsible for requirements and Systems Command is responsible for development and acquisition.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- HQMC issued Marine Corps Order 3430.5A, Policy for Command and Control Warfare (C2W). The Marine Corps is more comfortable with Command and Control Warfare than Information Warfare. C2W is better defined and oriented toward the tactical and operational levels of war and therefore more coincident with Marine Corps missions.
- A small force, the Marine Corps must leverage their funds and billets by taking advantage of Navy and other Service initiatives. For example, Marine billets in the FIWC, NIWA, the AFIWC, and the JC2WC, ensure they are “in the loop” and receive a share of the services provided by these organizations.
- Panels and Working Groups: HQMC has established an IW working group to coordinate IW activities between all HQMC departments, the Marine Corps Combat Development Command (MCCDC), and the operating forces.
- Protect: The Marine Corps is investigating ways to that COMSEC and C2W tools get down to the operating forces. Seventeen (17) firewalls are being implemented at the NIPRNET gateways to the USMC Banyan network.

- Detect and React: The Marine Corps is working with the FIWC; the home of the Navy Computer Incident Response Team, to receive emergency response support. The FIWC is scheduled to conduct on-line surveys, probes of Marine Corps networks and systems, this summer. The purpose of the survey is to establish a baseline of system vulnerabilities. Follow-up surveys are envisioned but on an as needed basis. Neither the Navy or Marine Corps plan to establish a Red Team organization.

This page intentionally left blank.


Department of the Air Force
Secretary of the Air Force
S. Widnall
Chief of Staff
Gen R. Fogleman
Air Combat Command
ACS Intelligence
Maj. Gen J. Casciano
Deputy Chief, Operations
Lt Gen Eberhart
Air Force Materiel Command
Deputy Chief of Staff C4
LtGen J. Fairfield
609th Air Operations Group
Air Intelligence Agency
Brig. Gen M. Hayden
Information Warfare Division (XOFE)
Col Lieberherr
Electronic Systems Center
Information Warfare Division (SCTW)
Col G. Fiedler
609th IW Squadron
Lt Col Rhoades
Air Force Information Warfare Center
Col Morgan
ESC/ICW
Capt L. Williams
Rome Laboratory
Air Force C4 Agency, IW Division
Mr. Goessman

Organization: Department of the Air Force

Senior Information Warfare Officials:

Lt Gen Ralph Eberhart, Deputy Chief of Staff for Plans and Operations
Lt Gen John S. Fairfield, Deputy Chief of Staff for C4I
Maj Gen John P. Casciano, Assistant Chief of Staff for Intelligence

Information Warfare Points of Contact:

Col Lieberherr, Information Warfare Division (XOFE), Office of the Deputy Chief of Staff for Plans and Operations
Col George Fiedler, Chief, Information Warfare Division (SCTW), Office of the Deputy Chief of Staff for C4I
Lt Col Blunden, Special programs Division (INXI), Office of the Assistant Chief of Staff for Intelligence
Howard Schmidt/John DeMaggio, Air Force Office of Special Investigations
Goessman, Information Protection Division, Air Force C4 Agency
Capt Lee Williams, Information Warfare Division (ICW), Electronic Systems Center
Maria Ramirez, AIA/XPR, Air Intelligence Agency
Feliciano Rodriguez, Air Force Information Warfare Center
John Pirog, IWT, Rome Laboratory
Lt Col Rhoades, 609th IW Squadron

On-Line Resources:

USAF Homepage: http://www.dtic.mil:80/airforcelink/

Information Warfare Related Organizations, Missions and Functions:

Deputy Chief of Staff for Operations (XO): XO has the lead for coordinating information warfare doctrine in the Air Force. XO has established an Information Warfare Division (XOFE) that leads the Information Dominance Panel directing $4 Billion in Air Force programs.

Deputy Chief of Staff for Communications and Information (SC): SC is responsible for orchestrating Information Protection (IP) efforts across the Air Force and for ensuring that IW and IP are considered in all planning efforts. SC has established an Information Warfare Division (SCTW).

> Air Force C4 Agency (AFC4A): AFC4A is responsible for developing C4 security policy.

Electronic Systems Center (ESC): ESC has established an IW Division which is responsible for selection, installation and sustainment of Base Information Protection Products.

Rome Laboratory, ESC, is establishing a single, integrated, laboratory-wide science and technology thrust for information warfare.

The Air Force Information Warfare Center (AFIWC) was established, in October 1993. An organizational summary for the AFIWC follows.

609th IW Squadron: The 609th is a prototype Information Warfare Squadron at Shaw AFB. Deployable AFIWC-type services will be provided by IW Squadrons.

Air Force Office of Special Investigations (OSI): OSI has established a computer forensics laboratory at Bolling Air Force Base.

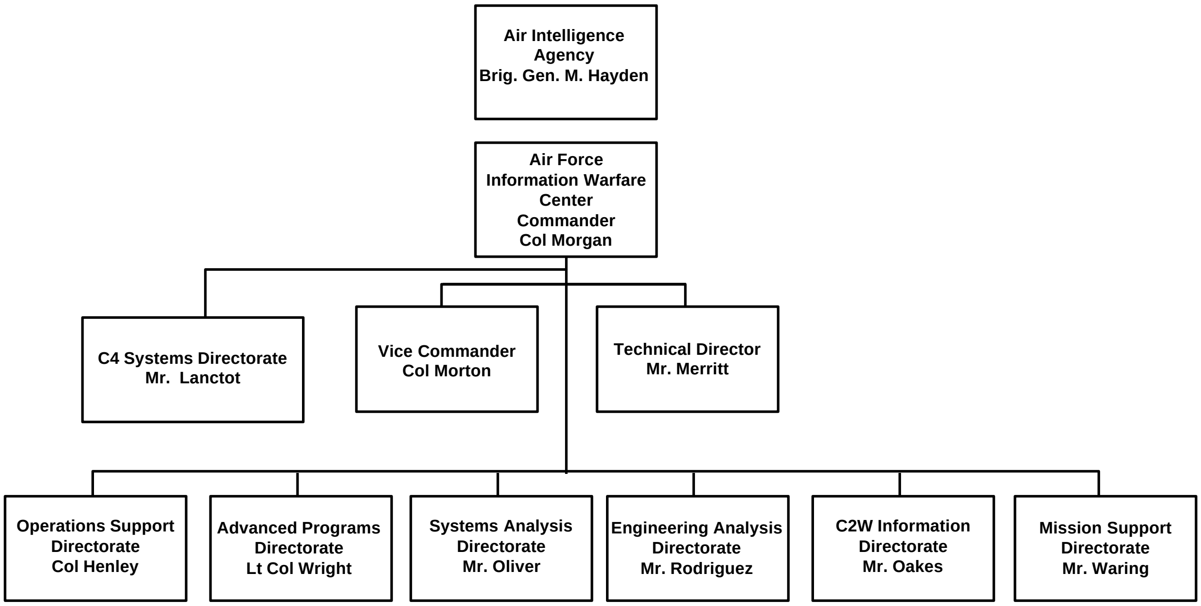
Due, in part, to the integrated, cross-cutting approach to IW within the Air Force, many line and staff organizations at various levels are actively involved integrating IW into Air Force doctrine, policy, plans, programs, and procedures. At the Air Staff, the operations, C4, intelligence, information management, acquisition, and security police communities participate in the Information Protection Working Group and other forums. Line organizations, such as the Air Force C4 Agency, Electronic Systems Command, the 38th EIW at Tinker AFB, and the Air Logistics Command in San Antonio are key contributors. MAJCOMs have assigned information protection (IP) responsibilities and Base Information Protection Offices have been established at the base level under Base Communications Squadrons.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- *Cornerstones of Information Warfare*, released in Aug 95, provides the Air Force doctrinal foundation as a first step toward integrating information warfare into Air Force doctrine. The concepts in *Cornerstones* are being incorporated into Basic Air and Space Doctrine of the United States Air Force (AF Manual 1-1). *Cornerstones* uses airpower terminology and examples to describe IW and proposes new Air Force missions of Counterinformation, C2 Attack, and Information Operations. The White Paper, *Air Force Information Protection Vision* , dated 25 April 1995, identifies an Information Protection (IP) strategy. A series of Air Force Instructions (AFI 33-2 series), covering all aspects of IP, have recently been revised or are in the process of being revised. ESCs Base Information Master Plan and the BNCC CONOPS address IP at the base level.
- Panels and Working Groups: The Air Force Corporate Board structure--a hierarchy of executive panels and steering groups--and the IW Technical Planning Integration Process Team (IWTPIPT)are key to integrating IW into Air Force operations, functions and organizations. The IWTPIPT uses a cost constrained, 25 year modernization planning process. The IWTPIPT is co-chaired by ESC and AFIWC. Within the Air Force Corporate Board structure, the C4I Panel, chaired by SC, and the Information Dominance Panel, chaired by XOFE, are the principal panels addressing IW issues. The INFOSEC Program Element, which, among other things, funds the AFIWC, falls under the Information Dominance Panel. Another key group at the Air Staff level, is the Information Protection Working Group (IPWG). Members include representatives from the Assistant Chief of Staff for Intelligence (IN), XO, SC, and representatives from the acquisition, information management, and security police communities. The principal

responsibility of the IPWG is coordination of Air Force wide efforts to protect Air Force information and automated information systems and processes. Base Information Protection Working Groups and Information Infrastructure Steering Groups also contribute to protection of the base infrastructures.

- Risk Management: The Air Force is a strong proponent of a risk management approach to IW-D. Through vulnerability and threat assessments, a risk management process is employed to provide appropriate protection based on operational priorities while considering economies of scale. The Air Force Risk Management Model, developed by the AFIWC, has been proposed for adoption by OSD.
- Protect: The Combat Information Transport System (CITS) is a base infrastructure upgrade program which provides a fiber optic backbone, base switches, and funds the BNCCs and security requirements. The FY 97 POM provides for 60% funding of the infrastructure programs and 100% of the security requirement. Support to deployed forces will be provided by Deployed Network Control Centers (DNCC) with a second tier of support at the AFFOR level. The Air Force is beta testing FORTEZZA and Armor Mail and is pursuing a MLS enclave beta test for the SC staff.
- Detect and React: The Base Network Control Center (BNCC) is the focal point for base network management and protection. Security tools to do self assessments; e.g., on-line surveys, automated network management, intrusion detection capabilities, are planned for integration into the BNCC. The first step provides free or low cost tools the BNCCs to quickly provide some measure of IP. The BNCCs are provided integrated network management and IP support from MAJCOM Network Support Centers, the Air Force Network Support Center and the AFIWC. The Air Force is also pursuing increased coordination between the AFIWC and other Service and Agency IW activities such as the DISA ASSIST, Army's LIWA and the Navy's NIWA.
- Training, Education and Awareness: The Air Force feels that training provides the greatest return on investment in IP. A Process Action Team (PAT) is looking at all levels of training. Professional Military Education programs are underway for O-6's and Flag Officers. Network Management Training is provided by Air Education and Training (AETC) Command at Keesler AFB. An initiative is also underway to incorporate IP training at the unit level.
- Legal: The Air Force General Counsel has completed a report on IW legal issues. The final report is classified.


Air Intelligence Agency
Brig. Gen. M. Hayden
Air Force Information Warfare Center Commander
Col Morgan
C4 Systems Directorate
Mr. Lanctot
Vice Commander
Col Morton
Technical Director
Mr. Merritt
Operations Support Directorate
Col Henley
Advanced Programs Directorate
Lt Col Wright
Systems Analysis Directorate
Mr. Oliver
Engineering Analysis Directorate
Mr. Rodriguez
C2W Information Directorate
Mr. Oakes
Mission Support Directorate
Mr. Waring

Organization: Air Force Information Warfare Center

Senior Information Warfare Officials:

Col Frank M. Morgan, Commander

Information Warfare Points of Contact:

Feliciano Rodriguez, Director, Engineering Analysis Directorate
Fred Ramirez, AFCERT

On-Line Resources:

AFIWC Homepage: http://www.aia.af.mil/hqaia/afiwc

Information Warfare Related Organizations, Missions and Functions:

AFIWC's mission is to develop, maintain, and deploy information warfare/command and control warfare (IW/C2W) capabilities in support of operations, campaign planning, acquisition, and testing. The Center acts as the time-sensitive, single focal point for intelligence data and C2W services. It provides technical expertise for computer and communications security (COMPUSEC/COMSEC) and is the Air Force's focal point for tactical deception (TD) and OPSEC training.

The Engineering Analysis (EA) Directorate supports information and weapon systems development by providing technical guidance in the areas of computer and communications security; supports Information Protect (IP) through management of the C4 Systems Security Assessment Program (CSAP) to improve the security posture of AF C4 systems; develops security countermeasures, specialized tools and provides security engineering consultant services; manages and operates the Air Force Computer Emergency Response Team (AFCERT); and serves as the C4 systems security technical office for IP product and field assessments, security test and evaluation, electromagnetic field and lab emission security and zone testing.

The Air Force Computer Emergency Response Team (AFCERT) was established by the Air Force Information Warfare Center as the single point of contact in the Air Force for reporting and handling computer security incidents and vulnerabilities. The AFCERT coordinates the technical resources of AFIWC to assess, analyze, and provide countermeasures for computer security incidents and vulnerabilities reported by Air Force computer users, security managers, and system managers. The AFCERT deploys incident response teams to recover networked computer systems under attack from unauthorized sources. AFCERT Advisories are furnished to all users providing the latest information on system vulnerabilities and applicable countermeasures. The AFCERT coordinates computer security-related activities with all outside agencies and provides technical support to the Air Force Office of Special Investigations (AFOSI) during criminal and counter-intelligence investigations.

The Countermeasures Engineering Team (CMET) is responsible for integrating and validating technical computer and network security solutions for identified operational security vulnerabilities. The CMET's technical successes experienced through the development of intrusion detection tools, e.g., DIDS and NSM, vulnerability testing techniques, e.g., OLS, and specialized support to the AFCERT's incident response and recovery operations, were due in large part to the research and countermeasure prototype activities analogous with CMET operations. The CMET also provides engineering expertise to the telephone switch vulnerability assessment program and identifies countermeasure solutions. The continued operation of the CMET allows quick corrective reaction to new vulnerabilities identified during AFCERT operations.

The Electronic Security Survey Team (ESST) is a key component of the Air Force Information Warfare Center's Command, Control, Communications, and Computer (C4) Systems Security Assessment Program (CSAP). The major objective of the ESST is to improve C4 systems security posture by measuring the effectiveness of organizational electronic security and recommending COMSEC, COMPUSEC, and TEMPEST countermeasures where deficiencies exist. The 67 Intelligence Wing (67IW) deploys ESSTs to conduct Electronic Security Surveys (ESSs) for Air Force commanders worldwide. The ESST performs a field assessment to measure and evaluate the current computer, communications, and TEMPEST security posture of an Air Force facility. ESS assessments are accomplished in two phases: low profile and high profile. During the low-profile phase, a physical evaluation of individual work stations is conducted. The focus of this phase is to find unauthorized software, passwords, review magnetic media labeling, unauthorized connectivity, and search for obvious computer security vulnerabilities. The purpose of the high-profile phase is to identify procedural vulnerabilities and gauge the level of C4 system awareness and training of assigned members. Identified vulnerabilities, recommended countermeasures, and a local area threat study are presented in the final report.

The Electronic Security Engineering Team (ESET) performs field surveys to measure and evaluate the current C4 system security posture of Air Force facilities. The survey teams identify technical vulnerabilities and recommend solutions. Engineering teams use a variety of automated security tools. These tools include: anti-virus products, Computer Oracle and Password System (COPS), password cracking tools, firewalls to block certain traffic to a protected network, Internet Security Scanner (ISS), Network Security Monitor (NSM), Security Profile Inspector (SPI), TCP Wrappers to monitor incoming network traffic, and TRIPWIRE to monitor a designated set of files for changes.

Security Technology Insertion and Test Team (STIT) provide technical support to MAJCOMs, SPOs, AFOTEC and field units for security solution, weapon system and C4I system development and test efforts. The STIT Teams will: (1) develop, test, and integrate security solutions for security deficiencies; (2) perform security product testing in support of solutions and customer requests (3) analyze new operating systems being used in new/upgraded weapon and C4I systems; and (4) perform vulnerability testing in support of security test and evaluation of acquisition/upgrade program efforts.

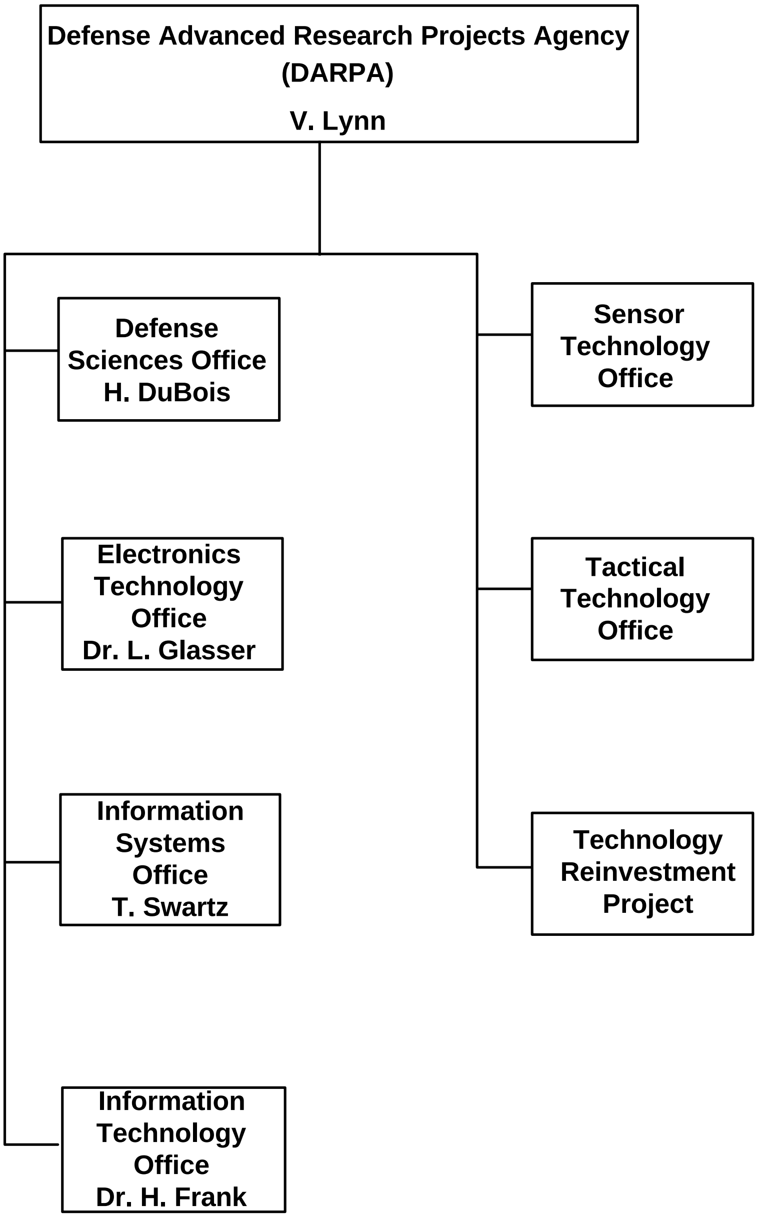
- A solution development team identifies solutions for documented security deficiencies in customers' networks. This team provides recommendations as well as prototyping and integration of solutions at customer site and/or in the EA technology LAB. This team assists in the development of secure network architectures for identified security deficiencies.
- Security product testing includes conducting product assessments in support of solution development, individual customer requests, or under direction from the Air Staff or AFC4A. Product testing includes functional security tests, vulnerability testing, and identification of security integration issues associated with the security products.
- Analysis of new/upgraded weapon and C4I systems that will be deployed within the Air Force and key operational systems. Analysis includes testing for existing security vulnerabilities, security weaknesses, and associated risks of fielding the operating systems within weapon and C4I systems with specific configurations and applications.
- Engineering teams assist SPOs, FOTEC, and other organizations with the conduct of ST&Es for specialized AF systems. This assistance will be for the specific purpose of performing vulnerability testing in support of security test and evaluation of acquisition/upgrade program efforts.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- The AFCERT conducts On-Line Surveys (OLS) to measure the security posture of Air Force Systems. Survey operators attempt to penetrate targeted systems using known vulnerabilities. These penetration attempts should be detected by system administrators and reported to the Air Force Computer Emergency Response Team (AFCERT). The OLS team analyzes all data generated from testing and creates a report. This report is distributed to the base commander of the targeted systems and the MAJCOM. The report describes the security weaknesses found on each system targeted and the associated countermeasure. The report also tells where the administrator needs to go for further information and help. The OLS results are used to steer Air Force efforts to strengthen Air Force C4 systems security.
- The Network Security Monitor (NSM) Program is designed to measure the level of unauthorized activity against Air Force C4 systems. The network traffic data from individual sites is reported to and centrally analyzed by the AFCERT every 24 hours. NSM analysts then measure the level of unauthorized activity using a Statistical Process Control (SPC) methodology. When network traffic analysis reveals suspected unauthorized activity using a Statistical Process Control (SPC) methodology. When network traffic analysis reveals suspected unauthorized activity, the AFCERT validates the data with the affected unit and initiates incident response measures. The AFOSI is informed and opens an investigation at the NSM site as appropriate. The AFOSI may request technical assistance from the AFCERT to support their investigation. NSM is currently operational at 38 sites and is approved for Air Force-wide installation by December 1997. There are two main areas of future development for NSM. First, portability to Linus-based personal computers and second, increasing user-friendliness of NSM's graphical interface with real-time data.

- The AFCERT manages the C4 Database System (CDS) that provides for complete documentation of Air Force computer security incidents, virus profiles, countermeasures, vulnerability testing, and network monitoring activities. The CDS affords the AFCERT on-line access to computer security statistical data that provides the security posture of networked computer systems Air Force wide. Future development includes CDS on-line access by AF Major Commands and Base Network Control Centers (BNCC).
- The Distributed Intrusion Detection System (DIDS) is designed to identify and report misuse of computer systems. It does so by tracking users, finding out where users are coming from, what they are doing, and looking for known patterns of misuse. It is designed as a tool to assist network administrators or Computer Systems Security Officers (CSSOs) in maintaining the security of their systems. DIDS provides the ability to track users across the network using the Network ID (NID). It identifies users despite changes in login names and remote logins to other computers and provides the network administrator or CSSO centralized access to network information about the security status of a system. The DIDS Director is the central computer which correlates the information it receives and produces human-readable reports for the CSSO. Each monitored host runs a host monitor which collects and analyzes audit records from the operating system. It looks for notable security-related events and sends them to the DIDS Director for further analysis. Future development includes a hierarchical DIDS Director to monitor wide area networks.
- The Information Protect Operations Decision Support System (IPODSS) is a new concept developed by the AFIWC that provides for the collection, integration and display of threat, vulnerability, and system data that will be used to quantify risks and develop courses of action (COAs) for Information Protection (IP) operations. Specifically, IPODSS will provide continuous status of IP posture, integrate indications and warning (I&W) support, and near-real-time (NRT) analysis and decision support for IP operations. Providing continuous status of the IP posture means monitoring and displaying system connectivity, vulnerability, threat, and performance data in NRT. The status of deployed and deployable IP assets (e.g., incident response teams) also should be monitored. IPODSS should be capable of distilling these data into overall assessments of the risk posture within an area of interest. Integrated I&W support means analyzing and correlating traditional and network-derived intelligence to facilitate more timely assessments of adversary intent and allow for prompt dissemination of appropriate warning and action messages. Traditional I&W includes detection of force deployments, increased communications, etc. Network-derived intelligence includes detections of system intrusions, assessments of likely targeted systems, etc. IPODSS should be capable of accessing and analyzing both structured and unstructured threat data (from traditional and emerging sources) to support timely I&W. The resulting assessments will be disseminated, along with directed COAs formulated via the analysis and decision support capabilities of IPODSS. Full realization of IPODSS analysis and decision support capabilities will require development and implementation of integrated operations centers. In the integrated operations center, data should be fused and correlated to support graphical display of the IO situation in operator-selectable regions. The decision support capabilities of the system should then allow rapid assessment of options (e.g., via sim/mod applications) to provide insight into projected outcomes. Intermediate analysis inputs,

situation tracks, responsive capabilities, and other operational data also should be available. Multi-function displays (MFDs) should be used to allow flexible, configurable display of operator-selected information. The IPODSS initiative is currently being coordinated with other Air Force and DoD agencies.


Defense Advanced Research Projects Agency
(DARPA)
V. Lynn
Defense
Sciences Office
H. DuBois
Electronics
Technology
Office
Dr. L. Glasser
Information
Systems
Office
T. Swartz
Information
Technology
Office
Dr. H. Frank
Sensor
Technology
Office
Tactical
Technology
Office
Technology
Reinvestment
Project

Organization: Defense Advanced Research Projects Agency

Senior Information Warfare Official:

Dr. Howard Frank, Director, Information Technology Office, DARPA

Information Warfare Points of Contact:

Ms. Teresa Lunt, Program Manager, ITO, DARPA

On-Line Resources:

DARPA Homepage: http://www.darpa.mil/
DARPA Information Survivability Homepage:
http://www.ito.darpa.mil/ResearchAreas/Information_Survivability.html

Information Warfare Related Organizations, Missions and Functions:

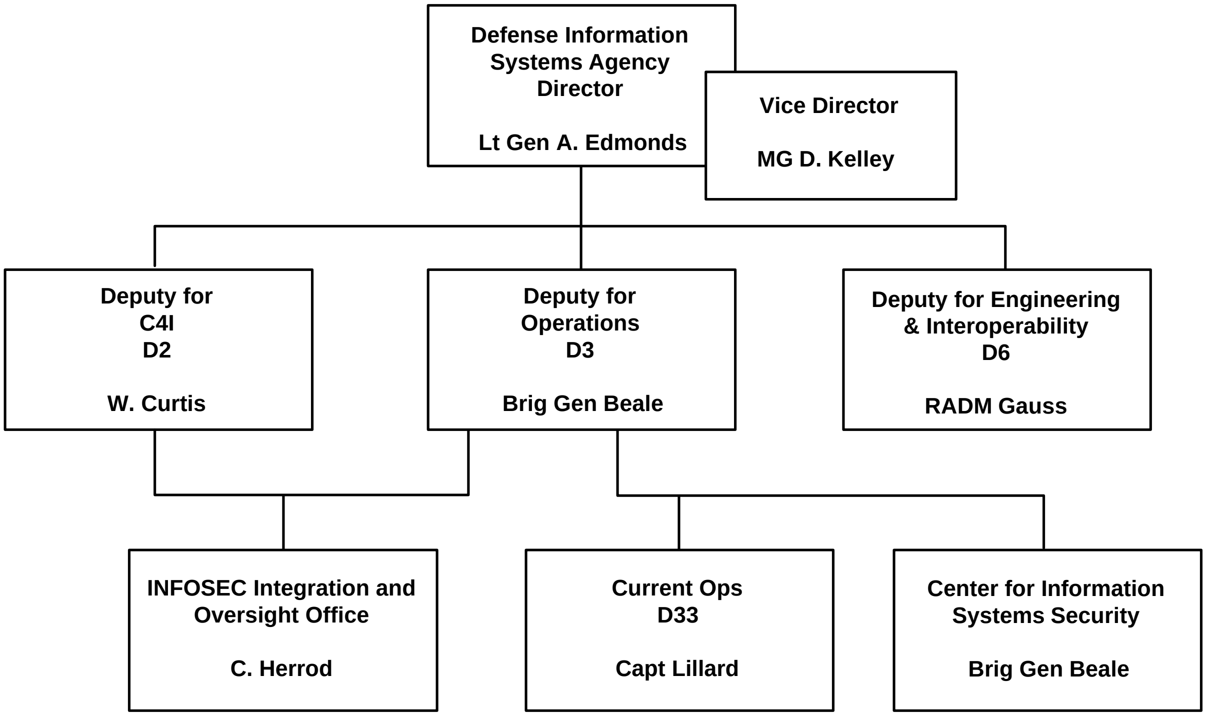
DARPA is responsible for advanced research in areas related to Defensive Information Warfare.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- DARPA is a co-founder, with DISA and NSA, of the Information System Security Research Joint Technology Office (ISSR-JTO). The ISSR-JTO was established to coordinate the information systems security research programs of DARPA and NSA. The ISSR-JTO works to optimize use of the limited research funds available, and strengthen the responsiveness of the programs to DISA, expediting delivery of technologies that meet DISA's requirements to safeguard the confidentiality, integrity, authenticity, and availability of data in DoD information systems, provide a robust first line of defense for IW-D, and permit electronic commerce between the DoD and its contractors.
- DARPA has renamed its Defensive Information Warfare program to Information Survivability. The Information Survivability program creates advanced technologies to protect DoD's mission-critical capabilities against electronic attack upon or through their supporting computing infrastructure. The goal is to create affordable, verifiable, scaleable technologies for a robust and secure defense infrastructure through configurable replaceable components and robust system design technology.
- The focus of the Information Survivability program is in the following four areas:
  - High Confidence Networking: Interoperable, scaleable, verifiable protocols and network security services to provide security and reliability to higher-level applications.
  - High Confidence Computing Systems: Modular, verifiable prototype systems with configurable replaceable components for security, reliability and real-time.
  - Assurance and Integration: Tools for designing, integrating and evaluating systems for security and robustness.

  - Survivability for Large Scale Information Systems: Techniques and tools to achieve survivability of large-scale defense infrastructure systems
- In 1995 DARPA sponsored a IW-D Summer Study to examine whether the nation's critical information infrastructure could be hardened to improve survivability against a wide range of possible threats. The following is a brief summary of the study's findings.
  - The systems that matter are often complex, unstructured, and include COTS and legacy components.
  - The process of hardening complex systems is poorly understood.
  - Laboratory successes are not impacting the nationally critical technologies.
  - The requirement: a practical technology for selectively hardening complex systems to achieve "high confidence" solutions.
- Robustness of systems must be widely defined. Two useful models can be found in biological and social systems. For example, a public health infrastructure could be created to immunize the population, and diversity would ensure that a population is not susceptible to a single attack.

This page intentionally left blank.


Defense Information Systems Agency Director
Lt Gen A. Edmonds
Vice Director
MG D. Kelley
Deputy for C4I D2
W. Curtis
Deputy for Operations D3
Brig Gen Beale
Deputy for Engineering & Interoperability D6
RADM Gauss
INFOSEC Integration and Oversight Office
C. Herrod
Current Ops D33
Capt Lillard
Center for Information Systems Security
Brig Gen Beale

Organization: Defense Information Systems Agency (DISA)

Senior Information Assurance Official:

Lt Gen Al Edmonds, Director, DISA

Information Assurance Points of Contact:

Brig Gen James Beale, USAF, Deputy Director for Operations (D3)
Chrisan Herrod, Chief, INFOSEC Integration and Oversight Office, Directorate of Operations (D3)
Sara Jane League, Deputy Director, Center for Information Systems Security (CISS)

On-Line Resources:

DISA Homepage: http://www.disa.mil/
DISA CISS Homepage: http://www.disa.mil/ciss/index.html

Information Assurance Related Organizations, Missions and Functions:

DISA's IW-D responsibilities are those specified by directives and those implied by DISA's responsibilities to centrally manage the DII. The following directives outline the specific responsibilities:

- Department of Defense Directive 3222.4, Electronic Warfare (EW) and Command and Control and Communications Countermeasures (C3CM), July 31, 1992, which charged the Director, DISA, to "... ensure that DISA architectures consider EW, ECCM, and C3CM."

- Department of Defense Directive 8000.1, Defense Information Management Program, October 27, 1992, which tasked the Director, DISA, to "... in consultation with the Directors of the Defense Intelligence Agency and the National Security Agency, provide technology and services to ensure the availability, reliability and maintainability, integrity, and security of defense information, commensurate with its intended use."

- Department of Defense Directive TS 3600.1, Information Warfare, December 21, 1992, which assigned responsibility to the Director, DISA, to "... ensure the DII contains adequate protection against attack."

- Chairman of the Joint Chiefs of Staff Memorandum of Policy (MOP) Number 30, Command and Control Warfare, 8 March 1993, which tasked the Director, DISA, to "... assess the vulnerabilities of ... defense information systems..." and to "maintain procedures to ensure a capability to respond to identified threats and assessed vulnerabilities."

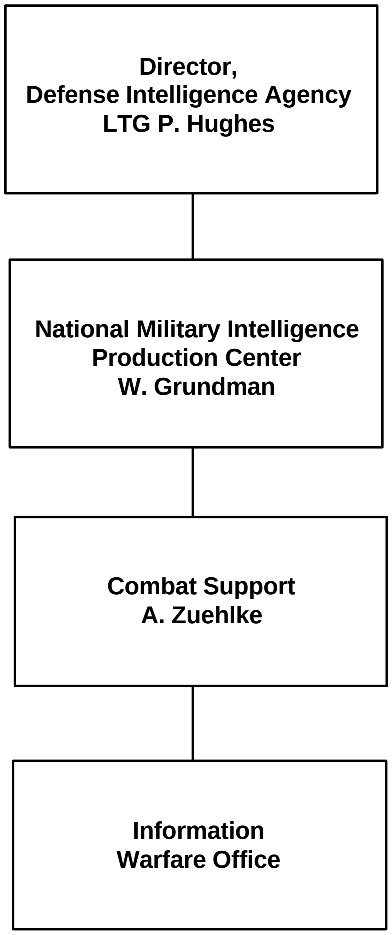
Formed in March 1996, the INFOSEC Integration and Oversight Office is jointly staffed by D2 and D3 with the function of overseeing the implementation of the DISA IW-D Management Plan, published 23 May 1996. The office will also develop the DoD IW-D Management Plan, assess the DII IW-D program, define DII protect, detect and react capability requirements, and develop performance goals and indicators and identify output measures for any assigned task.

DISA Center for Information Systems Security (CISS): The Center for INFOSEC (CISS), created by a Memorandum of Agreement between DISA and NSA on 12 May 1993, has the mission to develop and implement a Defense Information Warfare Program. The CISS is jointly manned by DISA and NSA personnel, in order to provide close coordination between the INFOSEC development and DoD implementor. The center was established as a DISA Field Operating Agency to support DoD, Joint and Service programs as required by DMRD 918 and to execute the Defense Information Systems Security Program (DISSP). To accomplish these key functions, CISS provides operational protection, detection, reaction and vulnerability analysis in support of the Defense Information Infrastructure; executes DoD requirements and processes for accreditation of computers, systems and networks; and develops, coordinates, and executes a DoD- wide INFOWAR education, training, and awareness program. CISS is also responsible for managing the INFOSEC Technical Services Contract and the DoD-wide Antivirus Software Initiative.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- In its simplest form, the DISA strategy for achieving a secure DII is based on three security pillars: protect the DII components and information from intrusions and disruptions (malicious and other); detect the intrusions and disruptions when they occur; and, react to intrusions and disruptions of the DII. The react capability will include the ability to: differentiate among malicious and other disruptions; warn the appropriate operators and users of the disruptions; isolate affected infrastructure components; reallocate infrastructure capabilities; and, recover and reconstitute the DII capability.
- The DISA Defensive Information Warfare (IW-D) Management Plan published on 23 May 1996, outlines the steps the Director, DISA will undertake to ensure the DISA-owned and managed and the DISA-managed portions of the DII are adequately protected against attack.
- DISA is currently working on obtaining the following capabilities for the DII:
    - Integrated network management and security management
    - Audit Monitoring and Detection System (AMIDS)
    - Malicious Code Detection Eradication System (MCDES)
    - Automated Infrastructure Management System (AIMS)
    - Vulnerability Analysis and Assessment Program (VAAP)
    - Integrated Security Operation Capability for the DII GCC/RCC
    - Personnel, Training, and Facilities
    - Wargames and Exercises
    - Reserve Component Utilization

- DISA is a co-founder, with DARPA and NSA, of the Information System Security Research Joint Technology Office (ISSR-JTO). The ISSR-JTO was established to coordinate the information systems security research programs of DARPA and NSA. The ISSR-JTO works to optimize use of the limited research funds available, and strengthen the responsiveness of the programs to DISA, expediting delivery of technologies that meet DISA's requirements to safeguard the confidentiality, integrity, authenticity, and availability of data in DoD information systems, provide a robust first line of defense for IW-D, and permit electronic commerce between the DoD and its contractors.
- The Special Budget Issue (SBI) on Information Systems Security (INFOSEC) approved by the Defense Resources Board (DRB) on September 19, 1995, and documented in Program Decision Memorandum (PDM) II provided significant funding for protecting the DII.
- The INFOSEC Technical Services Contract was awarded in July 1995. It is a five year, indefinite-delivery, indefinite-quantity contract which will provide INFOSEC services and products for the Federal government.


Director,
Defense Intelligence Agency
LTG P. Hughes
National Military Intelligence
Production Center
W. Grundman
Combat Support
A. Zuehlke
Information
Warfare Office

Organization: Defense Intelligence Agency (DIA)

Senior Information Warfare Official:

Arthur Zuehlke, Director, Directorate for Combat Support, National Military Intelligence Production Center

Information Warfare Points of Contact:

Michael Lamb, Information Warfare Office
Dr. John Yurechko, Information Warfare Office
Glenn Price, Information Warfare Office

On-Line Resources:

DIA Homepage: http://www.dia.mil

Information Warfare Related Missions and Functions:

Manage the Defense intelligence community production to support the full range of DoD information warfare activities.

Serve as the Defense intelligence community focal point for the development, management, and maintenance of information warfare data bases that facilitate timely dissemination of all-source, finished intelligence in support of DoD information warfare activities.

Oversee DoD requirements, and serve as the Defense intelligence community focal point, for the development, management, and maintenance of information systems that facilitate timely collection, processing, and dissemination of all-source finished intelligence for DoD information warfare activities.

As DoD human intelligence (HUMINT) manager, provide oversight, guidance, and direction to the Defense HUMINT service, consistent with DoD information warfare objectives.

Oversee management of DoD intelligence information systems to ensure information warfare-related security requirements are defined and implemented.

Assist Unified Combatant Commands with the development of command intelligence architecture planning programs that fully integrate information warfare support requirements.

Assist the Chairman of the Joint Chiefs of Staff in developing joint information warfare doctrine and tactics, techniques, and procedures.

Coordinate with the DoD Components to share information warfare techniques and information warfare-related intelligence.

Oversee the cost-effective development of select information models and simulations foe scenario development, training and exercises, and targeting; and incorporate information warfare functions in the overall command, control, communications, computers and intelligence functional model.

Provide the Chairman of the Joint Chiefs of Staff and the Unified Combatant Commands with the timely intelligence required for effective information warfare target selection and post-strike analysis.

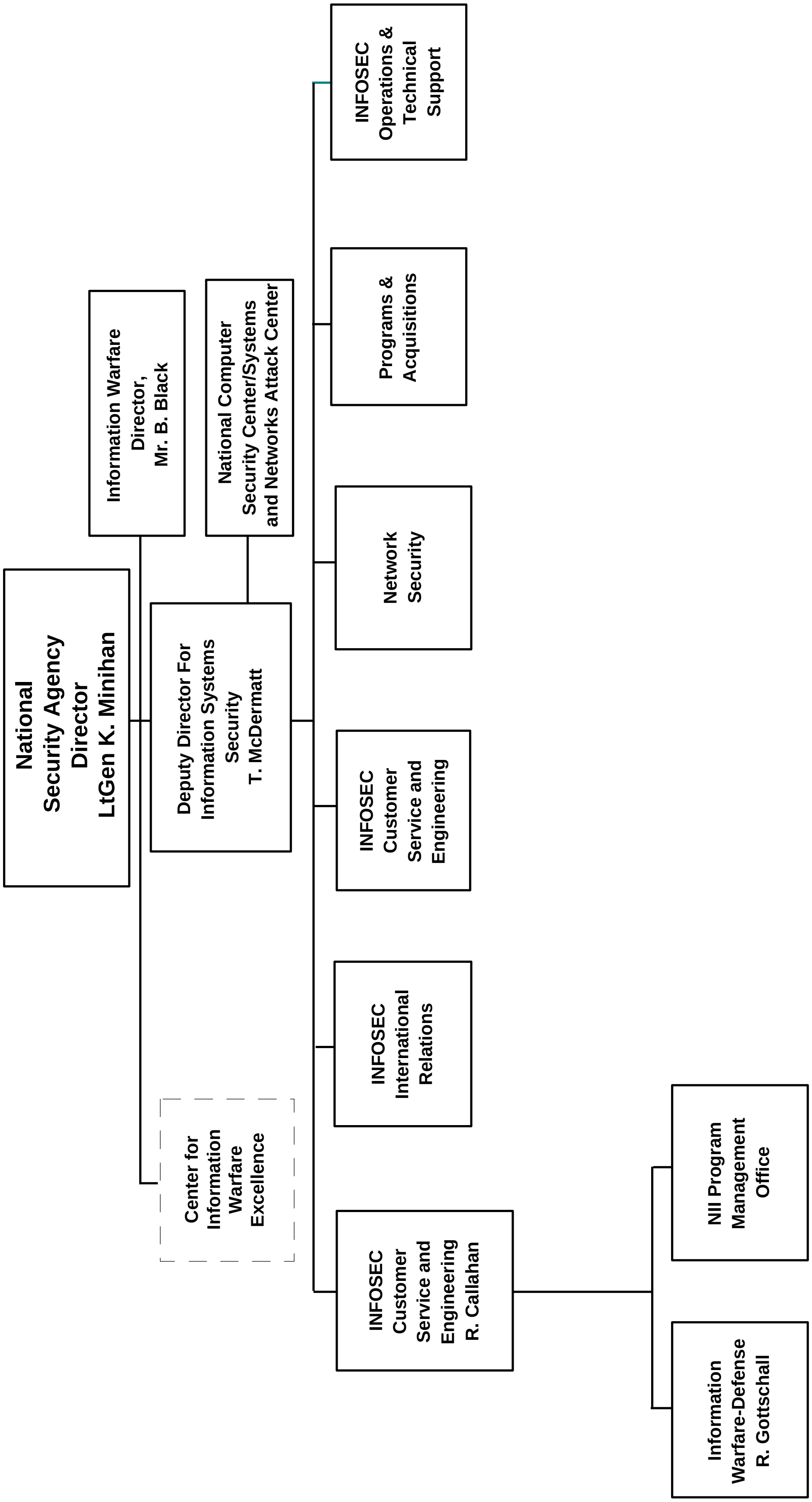
The DIA National Military Intelligence Systems Center is responsible for the certification and accreditation of DoD intelligence information systems and networks (excluding NSA systems).

DIA is responsible for development of foreign science and technology intelligence. In this role, DIA develops a strong awareness of foreign technology developments and transfers which could impact U.S. assets and capabilities.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- DIA has established an Information Warfare Office with a staffing level of 135 people.
- DIA is currently leading four key intelligence efforts:
  - With the advent of the information age and the threat posed by information warfare, the U.S. intelligence community must adopt a new approach to fulfilling its strategic and tactical indications and warning responsibilities, Conventional indications and warning mechanisms, procedures, and protocols may not suffice for information warfare. DIA, responsible for providing indications and warning of foreign military attacks against the U.S. and its interests, is leading a U.S. government-wide effort to ensure the challenges presented by information warfare are met fully by both the DoD and the National Indications and Warning Communities.
  - DIA chairs a U.S. government-wide forum, the Interdepartmental Information Warfare Threat Working Group, to exchange and discuss relevant threat information.
  - DIA has also established the Information Warfare Working Group to define a process and procedures for the coordination and production of threat assessments for information warfare-related activities.
  - DIA is developing an Information Warfare Support System (IWSS) to permit the complete integration of all Defense Intelligence Community IW-related software programs and serve as a single source of IW intelligence throughout the globe for producers and consumers alike.

This page intentionally left blank.


National Security Agency Director LtGen K. Minihan
Information Warfare Director, Mr. B. Black
National Computer Security Center/Systems and Networks Attack Center
Deputy Director For Information Systems Security T. McDermatt
Center for Information Warfare Excellence
INFOSEC Operations & Technical Support
Programs & Acquisitions
Network Security
INFOSEC Customer Service and Engineering
INFOSEC International Relations
INFOSEC Customer Service and Engineering R. Callahan
NII Program Management Office
Information Warfare-Defense R. Gottschall

Organization: National Security Agency

Senior Information Warfare Official:

Bill Black, Director of Information Warfare

Information Warfare Points of Contact and Areas of Interest:

Dr. Clint Brooks, Information Strategy

On-Line Resources:

NSA Homepage: http://www.nsa.gov:8080/

Information Warfare Related Missions and Functions:

The Director of Information Warfare reports to the Director, NSA for Information Warfare issues. He has broad coordination responsibilities to monitor Information Warfare-related activities in both DoD and non-DoD government departments and agencies. He represents the interests of NSA across the entire spectrum of functional disciplines which impact on Information Warfare.

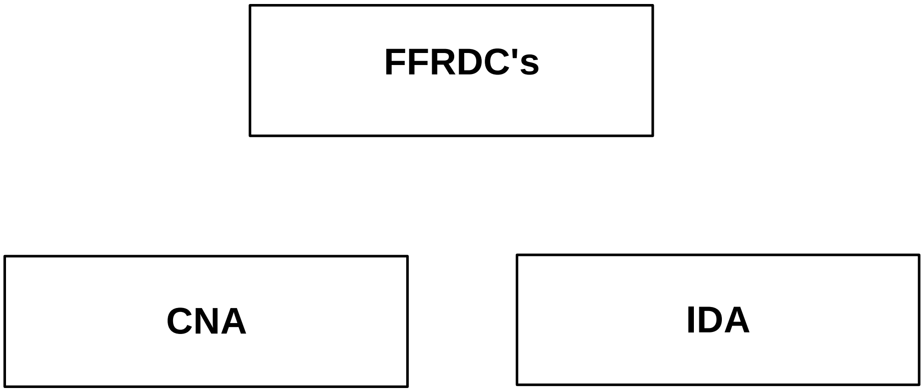
Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- Defensive information warfare or information assurance activities are not yet well defined. The lack of definition is nowhere more apparent (in NSA's eyes) than when viewed through the Computer Security Act of 1987 (P.L. 100-235). The Act stipulates (in part) that government classified information systems-based data is the responsibility of NSA, while government unclassified information is the responsibility of NIST. The difficulty arises when one considers that 95+% of (classified or unclassified) communications is transmitted across public switches, and the quantity of computers which are in the public domain.
- NSA has developed a concept through which NSA will respond to issues of personal privacy, business privacy, law enforcement, and foreign intelligence with its well-founded systems security expertise. An example of an initiative being promoted to address these issues is the key escrow concept.
- The legal ramifications of IW are significant. On the offensive side, roles are fairly clear after the beginning of hostilities. Before hostilities, deconfliction is a big issue. On the defensive side, P.L. 100-235 is a big issue. What constitutes computer crime? Legal issues at the national level are murky at best. On the international level, it gets murkier.
- NSA responsibilities include SIGINT, INFOSEC, and OPSEC.
- There is a Professional OPSEC Society which promotes OPSEC in the private sector.
- The National Computer Security Center and the Information Systems Security Organization provide a variety of products and services to DoD and the Federal government. Services include threat analysis, research and technology development,

system security assessments and evaluations and system security engineering. Products include a variety of items being developed under the Multilevel Information Systems Security Initiative (MISSI) program.

- The National Computer Security Center is working in conjunction with the National Institute of Standards and Technology and several other nations (among them Canada, France, Germany, and the Netherlands) to develop a new set of guidelines called the Common Criteria. It is hoped by NSA and NIST that the Common Criteria will eventually replace the Orange Book (i.e., Trusted Computer Systems Evaluation Criteria).
- A Systems and Networks Attack Center (SNAC) was formed in May 1995 to replace portions of the National Computer Security Center. This center identifies systems and network vulnerabilities and network attack technologies.
- NSA has integrated the Information Systems Security Organization mission into the National Security Operations Center.
- NSA is in the process of establishing an Information Warfare Center of Excellence. This center will be jointly staffed by NSA, DIA, CIA, and others. It will focus on threats, vulnerabilities, and indications and warning.
- NSA is focused on the Global Information Infrastructure.

This page intentionally left blank.



FFRDC's

CNA

IDA

Organization: Center for Naval Analyses (CNA)

Senior Information Warfare Officials:

Ambassador Linton F. Brooks, Vice President, Policy Strategic Forces Division

Information Warfare Point of Contact:

Dr. Gary A. Federici

On-Line Resources:

Information Warfare Related Organizations, Missions and Functions:

CNA is a federally funded research and development center (FFRDC) serving as a center of inquiry for its sponsor, the Department of Navy. As an independent source of applied research and policy analysis, CNA assists senior leaders of the U.S. Navy and Marine Corps by conducting a continuing program of objective analysis and practical evaluations of naval operations, systems, and programs. CNA conducts analyses for other government organizations when the research is directly related to CNA's purpose, mission, and areas of expertise. For information warfare, CNA has focused on the following issues: (1) the key information warfare roles likely to be entrusted to the Navy; (2) what the Navy must do to adequately prepare itself to perform those roles; (3) how the future defense environment, including operations other than war, should drive the Navy's approach to information warfare; (4) evaluation of alternative information architecture that will support future operating forces; and (5) JWCA analytical support to the Joint Staff (J38/J6K).

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- CNA has conducted:
  - Evaluations of the role Information Operations and Warfare plays in joint training exercises.
  - Concept demonstrations of new approaches to using information systems in combat environments.
  - Classified IW technology evaluations.
  - Studies of service roles and missions.
- Key issues addressed were:
  - Approaches to defensive appliqués concept.
  - Peacetime planning for executing IW.
  - Approach to quantify contributions of IW.
  - Roles, missions, and functions.
  - National IW policy issues: gaps and opportunities.
  - Mission planning and organizing for IW.
  - Intelligence support to IW.

- CNA approaches all analytical issues by using empirical data, when possible. No modeling and simulations technology are employed. Field demonstrations and interaction with operations are the norm.
- Lessons learned are available through CNA points of contact.

Organization: Institute for Defense Analyses (IDA)

Senior Information Warfare Official:

Information Warfare Points of Contact:

Terry Mayfield, Computer Software and Engineering Division
Bill Barlow, Systems Engineering Division
Robert Anthony, Operational Evaluation Division

On-Line Resources:

IDA Homepage: http://www.ida.org/

Information Warfare Related Missions and Functions:

DoD Studies and Analyses

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- In 1995, DARPA sponsored a IW-D Summer Study to examine whether the nation's critical information infrastructure could be hardened to improve survivability against a wide range of possible threats. IDA contributed to this study. The following is a brief summary of the study's findings.
  - The systems that matter are often complex, unstructured, and include COTS components.
  - The process of hardening complex systems is poorly understood.
  - Laboratory successes are not impacting the nationally critical technologies.
  - The requirement: a practical technology for selectively hardening complex systems to achieve "high confidence" solutions.
- As a part of its Joint Warfare Capability Assessment of Information Warfare, the Joint Staff (J6K) requested the Institute for Defense Analyses (IDA) to research, analyze, and evaluate open systems technologies within the DoD and private industry to baseline IW technology. The results of that effort are documented in IDA Document D-1792, *Information Warfare Technologies: Survey of Selected Civil Sector Activities*, February 1996, and IDA Paper P-3157, *Information Warfare: Selected Long-Range Technology Applications*, February 1996.
- The IDA Document identifies 56 technologies with potential information warfare application and for each technology describes the technology strengths and weaknesses, possible concepts of operation, potential risks and related information such as technology availability, points of contact, and patent or proprietary aspects
- Three IDA organizations support IW-related activities, the Systems Engineering Division, Operational Evaluation Division, and the Computer and Software Engineering Division.

- IDA has been asked by J6K to address the role and impact of industry in defensive information warfare. They will also research technologies in or out of DoD which have potential application information warfare.
- IW-related activities include:
  - Supported JS/J38 in concepts development leading to CJCS MOP 30, Command and Control Warfare.
  - Analysis of counter-drug operations and security policy development and labeling of information to control dissemination of the counter-drug information.
  - Estimating value of information and cost of security within DoD. Currently attempting to extend approach to estimate cost of security in private sector.
  - Ten years supporting NSA in developing trusted computer systems evaluation criteria and evaluating commercial products against such criteria.
  - Drafted distributed systems functional evaluation criteria for NSA.
  - Developed security labeling analysis for DoD Common Security Label standard which supports network operations. Counter-drug operational experience was used to add realism to the standard.
  - Drafted study of baselining and implications of DoD Goal Security Architecture.
  - Assistance to NSA in drafting, review, and editing of the entire Rainbow series of documents.
    - Studying viability of DGSA concepts in commercial operating systems.
    - Studying viability of wrapper concept in Systems Security Architecture.
    - Provided distributed systems portions to Common Criteria (CC); Drafting Protection Profiles for use in evaluating CC.
  - Assisting NSA in revitalizing INFOSEC Education, Training, and Research Programs.
  - Synthesized integrity aspects of INFOSEC into NCSC Technical Reports 79-91 and 101-91.
  - In cooperation with NSA and the U.S. Naval Postgraduate School, IDA is establishing a Center of Excellence for Information Security. USNPGS point of contact is Dr. Cynthia Irvine.
  - Supported NSA and DISA in developing harmonized certification and accreditation procedures for DoD information systems.
  - Supported DISA in developing the DoD Goal Security Architecture (DGSA) which identifies where to establish security and the supporting rationale, and in developing the DGSA Overall Transition Strategy which integrates security functions identified in the DGSA and organizational responsibilities.
  - Provided support to DISA Center for Standards on DGSA Transition Activities involving Standards.
  - Assisted DARPA is developing a BAA on Information Security (95-15) and in evaluating the proposals. Approximately 150 proposals were received for the program which begins in FY 96 and will continue for three years. This program will address protection of operating systems, firewalls, intrusion detection, infrastructure protocols, infrastructure vulnerabilities, cryptography, and assurance tools and techniques.

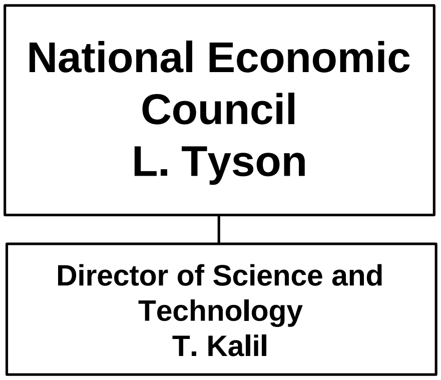
  - Assisted DARPA in developing a BAA for Information Survivability (BAA 96-03) which addresses technologies for a robust information infrastructure (consistency, distributed monitoring, staging of levels of protection, etc.).
  - Supported Office of Net Assessment in ongoing DIW Assessment (95-96).
  - GEN Larry Welch (President) appointed to Security Policy Advisory Board in 1996.
  - Have developed and conducted training and education courses on computer security.
  - Operate supercomputing research center in support of NSA. Have additional high performance computing research underway at LaJolla, CA, and Princeton, NJ.
  - Operate a simulation center. Attempting to define how to simulate the effects of IW.
- Conducted DARPA-sponsored invited workshops on Security in Optical Systems, Survivability, and Security in next-generation Command and Control Systems.
- Completed a Central Research Project on IW to identify and examine concepts and relevant activities associated with DoD initiatives. Paper intended to provide a foundation and starting point from which to address issues of requirements, strategy acquisition and implementation.
- Conducted analysis and review for the Commission on Roles and Missions of the Armed Forces (CORM) on IW concepts and linkages to Command, Control, Communications & Intelligence (C3I) topics and issues.
- Provides analyses for the Joint Staff (JS) of the conduct and lessons learned with respect to IW and Command & Control Warfare (C2W) during the extensive Bosnia air operations campaign from 1992-1995.

This page intentionally left blank.

Executive Branch

Executive Branch

This page intentionally left blank.



National Economic Council
L. Tyson

Director of Science and Technology
T. Kalil

Organization: National Economic Council (NEC)

Senior Information Assurance Official:

Hon. Laura Tyson, Assistant to the President for Economic Security

Information Assurance Points of Contact:

Tom Kalil, Director of Science and Technology, NEC Staff

On-Line Resources:

NEC Homepage: http://www1.whitehouse.gov/WH/EOP/nec/html/main.html

Information Assurance Related Missions and Functions:

The NEC was created by Executive Order on January 25, 1993. Its primary functions are to:

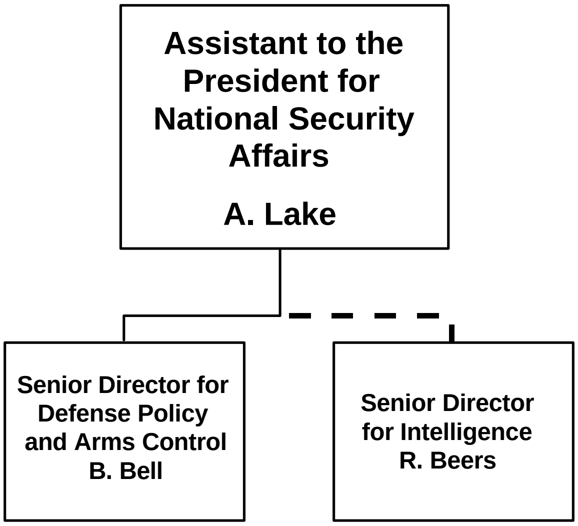
> Coordinate the economic policy-making process with respect to domestic and international economic issues.
>
> Coordinate economic policy advice to the President.
>
> Ensure the economic policy decisions and programs are consistent with the President's stated goals and to ensure that those goals are being effectively pursued.
>
> Monitor implementation of the President's economic policy agenda.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

The NEC and the Office of Science and Technology Policy collaborated on planning for the Information Infrastructure Task Force, which was established by Vice President Gore and is chaired by Hon. Ron Brown, Secretary of Commerce. Mr. Kalil continues to be actively involved in IITF activities.

Mr. Kalil is also involved in cryptology policy issues such export controls and key escrow considerations.

National Security Council Staff



Assistant to the President for National Security Affairs

A. Lake

Senior Director for Defense Policy and Arms Control
B. Bell

Senior Director for Intelligence
R. Beers

Organization: National Security Council (NSC) Staff

Senior Information Assurance Official:

Bob Bell, Senior Director for Defense Policy and Arms Control, NSC

Information Assurance Points of Contact:

CAPT Joe Sestak, Director for Defense Policy, NSC Staff
Randy Beers, Senior Director for Intelligence, NSC Staff
Ed Appel, Director for Counterintelligence, NSC Staff

On-Line Resources:

NCS Homepage: http://www.whitehouse.gov/WH/EOP/html/other/NSC-plain.html

Information Assurance Related Missions and Functions:

Members are the President, the Vice President, the Secretary of State, and the Secretary of Defense. The Director of Central Intelligence and the Chairman of the Joint Chiefs of Staff are statutory advisors for intelligence and military matters, respectively.

The Secretary of the Treasury, the U.S. Trade Representative, the Chief of Staff to the President, and the Assistants to the President for National Security Affairs and Economic Policy are invited to all meetings of the Council.

The Council advises and assists the President in integrating all aspects of national security policy as it affects the United States -- domestic, foreign, military, intelligence, and economic -- in conjunction with the National Economic Council.

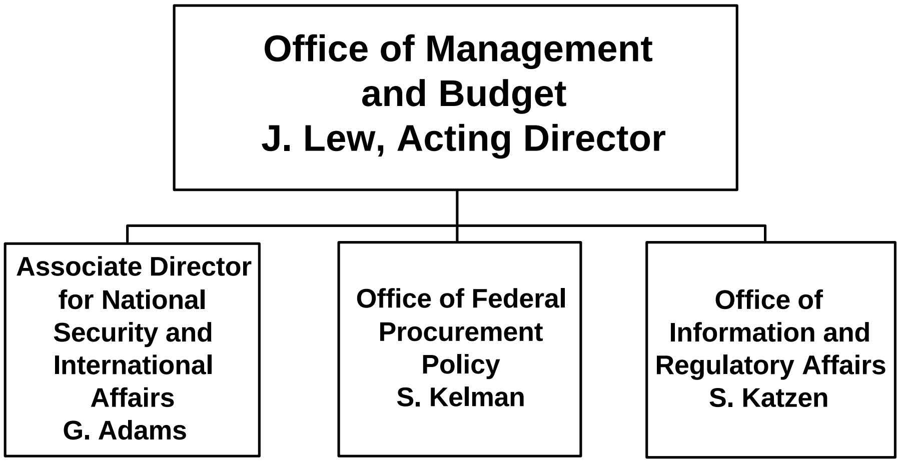
Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Defense Policy and Arms Control Office headed by Bob Bell has the lead for information operations and assurance.
- The Intelligence Office headed by Randy Beers handled the Clipper and data encryption issues. Mr. Ed Appel of this office also has oversight over the U.S. Security Policy Board.
- The 1995 national security strategy includes economic security which has implications in terms of roles and responsibilities for infrastructure protection and information assurance. In addition, the 1996 strategy includes the following statement:

> “Finally, the threat of intrusions to our military and commercial information systems poses a significant risk to national security and is being addressed.” [A National Security Strategy of Engagement and Enlargement, The White House, February, 1996]

- NSC initiated a review of the policy formulation process associated with information assurance and infrastructure protection. The results of that review will be implemented soon.
- The President's National Security Telecommunications Advisory Committee (NSTAC) asked for a focal point for information assurance in March 1995. The National Security Advisor was named as the focal point and is assisted in this role by the Senior Director for Defense Policy and Arms Control and his staff.

This page intentionally left blank.


Office of Management and Budget J. Lew, Acting Director
Associate Director for National Security and International Affairs G. Adams
Office of Federal Procurement Policy S. Kelman
Office of Information and Regulatory Affairs S. Katzen

Organization: Office of Management and Budget

Senior Information Assurance Official:

Sally Katzen, Administrator, Office of Information and Regulatory Affairs

Information Assurance Points of Contact:

Bruce McConnell, Chief, Office of Information and Regulatory Affairs
Ed Springer, Office of Information and Regulatory Affairs

On-Line Resources:

OMB Homepage: http://www.whitehouse.gov/WH/EOP/omb

Information Assurance Related Missions and Functions:

The Office of Management and Budget evaluates, formulates, and coordinates management procedures and program objectives within and among Federal departments and agencies. Some of its primary responsibilities are to assist the President in developing and maintaining effective government, assist in developing efficient coordinating mechanisms to expand interagency cooperation, assist the President in preparing the budget, assist in developing regulatory reform proposals and programs for paperwork reduction, especially reporting burdens of the public, to plan and develop information systems that provide the President with program performance data, and to improve the economy, efficiency, and effectiveness of the procurement process.

The Office of Management and Budget establishes Federal policy for the security of Federal automated information systems in OMB Circular No. A-130. Appendix III of the Circular requires Federal agencies to establish computer security programs and sets minimum requirements for such programs. The circular applies to the activities of all agencies of the Executive Branch. A revised Circular No. A-130 was distributed in February 1996 that included significant changes to Appendix III. National security information and national security emergency preparedness activities are subject to additional regulations under appropriate directives and executive orders.

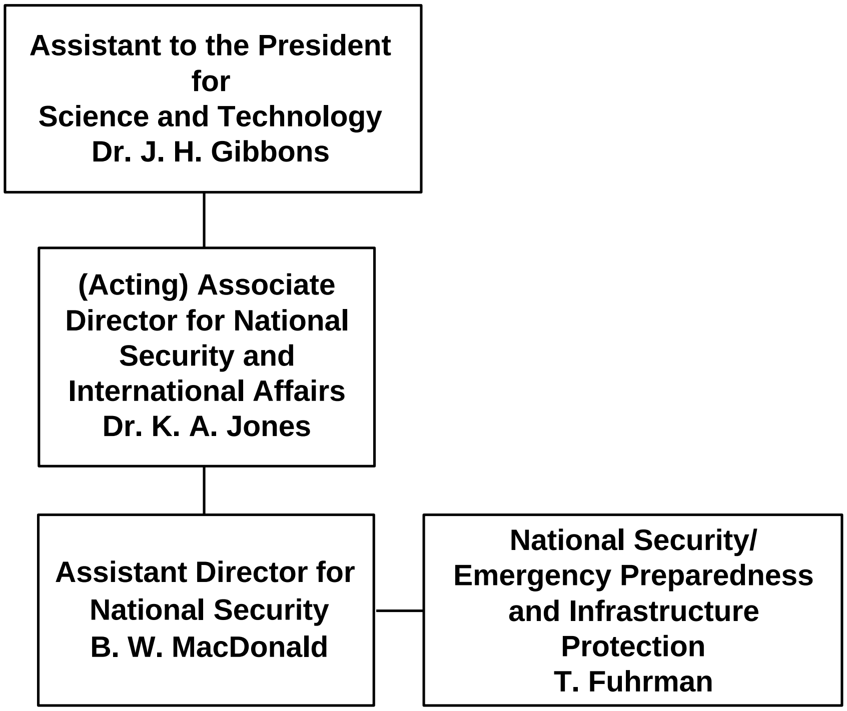
OMB Circular No. A-130, Management of Federal Information Resources, is issued pursuant to OMB's authorities under the Paperwork Reduction Act, (44 U.S.C., Chapter 35), the Privacy Act (5 U.S.C. 552A), the Chief Financial Officers Act (31 U.S.C. 3512 et seq), the Federal Property and Administrative Services Act (40 U.S.C. 759 and 487), the Computer Security Act (40 U.S.C. 759 note), the Budget and Accounting Act (31 U.S.C. Chapter 11), Executive Order 12046 and Executive Order 12472

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The OMB mission for infrastructure assurance is to ensure that all stakeholders are involved in the dialogue from the beginning. This is difficult because infrastructure assurance cuts across so many sectors and interests, but public participation is essential if infrastructure protection efforts are to succeed.
- Government doesn't own the infrastructure, therefore protection often requires regulation and participation from the public sector.
- A-130 Appendix III (security appendix) has been updated.
  - There is no longer a requirement for an agency information security official.
  - There is no longer a requirement to certify the security controls in sensitive applications.
  - There is no longer a requirement for an agency-level information security program; training is now required to be specific for systems.
  - The requirement for the performance of formal risk analysis, as an element of an agency information security has been deleted. The requirement is for management of risk rather than measurement of risk.
  - There is a new requirement for the incident response capabilities at the system level.
  - A new requirement for the inclusion of a summary of agency security plans in the information resources management plan required by Paperwork Reduction Act.
- The goal of the A-130 revision was to ensure that security is built into management control. Security is a personnel and management issue and A-130 imbeds security as a responsibility for both employees and managers. It recognizes the human aspect of security.
- OMB is a member of the Critical Infrastructure Working Group. The group has been established administratively, but funding has impacted performance.
- OMB now co-chairs the Inter-Agency Working Group on Cryptography.
- There is increased citizen awareness of information technology and of government information technology activity.
- Policy areas of concern include: intellectual property rights, software protection privacy, security (NII Security Plan due out shortly).
- National Performance Review implementation underway through Government Information Technology Services (GITS).

This page intentionally left blank.

Office of Science and Technology Policy


Assistant to the President for Science and Technology Dr. J. H. Gibbons
(Acting) Associate Director for National Security and International Affairs Dr. K. A. Jones
Assistant Director for National Security B. W. MacDonald
National Security/ Emergency Preparedness and Infrastructure Protection T. Fuhrman

Organization: Office of Science and Technology Policy (OSTP)

Senior Information Assurance Officials:

Dr. Kerri-Ann Jones, Acting Associate Director for National Security and International Affairs
Bruce MacDonald, Assistant Director for National Security

Information Assurance Points of Contact:

Tom Fuhrman, National Security and International Affairs Division
Dr. Mike Nelson, Special Assistant for Information Technology

On-Line Resources:

OSTP Homepage: http://www.whitehouse.gov/OSTP.html

Information Assurance Related Missions and Functions:

The Office of Science and Technology Policy (OSTP) was established by the National Science and Technology Policy, Organization, and Priorities Act of 1976 (Public Law 94-282). OSTP's responsibilities are to:

- Advise the President in policy formulation and budget development on all questions in which science and technology (S&T) are important elements.
- Lead an interagency effort to develop and implement S&T policies and budgets that are coordinated across Federal agencies.
- Articulate the President's S&T policies and programs to the Congress, and address and defend the need for appropriate resources.
- Foster strong partnerships among Federal, State, and local governments, and the scientific communities in industry and academe.
- Further international cooperation in science and technology activities.

OSTP's Director also serves as the Assistant to the President for Science and Technology. In this capacity, he manages the National Science and Technology Council (NSTC) and the President's Committee of Advisors on Science and Technology (PCAST).

The NSTC is a Cabinet council, chaired by the President, that acts as a "virtual" agency for science and technology to coordinate the diverse parts of the Federal R&D enterprise. PCAST is a committee of distinguished individuals appointed by the President to provide private sector advice in the S&T policy making process.

OSTP is led by a Director and four Associate Directors, all of whom are Presidentially-appointed and Senate-confirmed. OSTP is organized into four divisions:

Science Division

The Associate Director for Science leads the White House effort to ensure that: 1) the United States continues to maintain global leadership in science, mathematics, and engineering research; and (2) science continues to provide support for the successful resolution of some of the most important problems in the areas of health, agriculture, the economy, energy, social well-being, education, and national security. The Division focuses on maintaining a broad Federal research program that advances the frontiers of knowledge, is based on excellence, strongly coupled to education, and supportive of critical national goals.

Technology Division

The Associate Director for Technology leads the White House effort to develop and implement federal policies for harnessing technology to serve national goals such as global economic competitiveness, environmental quality, and national security. The Division's priorities include: redirecting the U.S. space and aeronautics program, including the space station; sustaining U.S. leadership in defense technology while increasing the focus on dual use and civilian technologies; advancing technologies for education and training for all learning environments; and facilitating development and adoption of advanced manufacturing technologies and advanced computing and communications technologies.

Environment Division

The Associate Director for Environment leads the White House efforts to: 1) ensure a sound scientific and technical underpinning for environmental policies, and 2) develop an interagency R&D strategy for environment and natural resource issues.

National Security and International Affairs Division

The Associate Director for National Security and International Affairs leads the White House effort to use science and technology in the service of our national security, and to shape and coordinate international cooperation in S&T. The national security agenda includes: defense technology investments in an era of downsizing; technical aspects of arms control and nonproliferation policy; technology transfer and related export control policies; and intelligence technology. The international agenda includes: using U.S. leadership in S&T to support U.S. foreign policy objectives; strengthening American S&T in the context of an increasingly interdependent world; using international cooperation in S&T to support economic goals; and enhancing international cooperation in large-scale science programs. The Associate Director for National Security and International Affairs also serves as the Senior Director for Science and Technology of the National Security Council staff.

OSTP also plays a key role in formulating a national strategy to advance the development and evolution of the National Information Infrastructure.

In addition, the National Security and International Affairs Division is responsible for all of OSTP's activities in the areas of national security/emergency preparedness, emergency telecommunications, the National Communications System, the National Security Telecommunications Advisory Committee, Continuity of Government programs and infrastructure protection programs, and works closely with the Technology Division on national information infrastructure issues.

OSTP has official responsibilities in protecting the domestic infrastructure deriving both from statute and executive order. As a result OSTP is in a unique position to bridge the cultural divides existing between the military and non-military sectors within the government, between the technical and the policy-making communities, and between the Federal government and state and local governments. The following activities are representative of the major responsibilities of OSTP:

> Statutory Role of OSTP. By statute, OSTP serves as a "source of scientific and technological analysis and judgment for the President with respect to major policies, plans, and programs of the Federal government." The statute further states that the Director of OSTP shall "seek to define coherent approaches for applying science and technology to critical and emerging national and international problems and for promoting coordination of the scientific and technological responsibilities and programs of the Federal departments and agencies in the resolution of such problems." (42 USC 6614)
>
> Emergency Telecommunications Authorities. By Executive Order, the OSTP Director is assigned responsibility for directing the exercise of the President's wartime authorities over domestic telecommunications which derive from the Communications Act of 1934. In emergencies or crises in which the exercise of the President's war power functions is not required or permitted by law, the OSTP Director is charged with the responsibility to advise and assist the President and Federal departments and agencies with the provision, management, or allocation of telecommunications resources. The National Communications System (NSC), a formal interagency organization, assists the President, the OSTP Director, the National Security Advisor, and the Director of OMB in the exercise of national security and emergency preparedness telecommunications functions. (47 CFR 201,202)
>
> Responsibilities under the Federal Response Plan. The Robert T. Stafford Disaster Relief and Emergency Assistance Act provides the authority to the Federal government to respond to disasters and emergencies in order to provide assistance to save lives and protect public health, safety, and property. The Federal Response Plan is designed to address the consequences of any disaster or emergency situation in which there is a need for Federal response assistance under the authorities of the Stafford Act. OSTP is responsible for the communications portion of the Federal Response Plan, which addresses Federal telecommunications support to federal, state, and local response efforts following a Presidentially declared emergency, major disaster, extraordinary situation, or other emergency. (42 USC 5121)

National Security Telecommunications Advisory Committee (NSTAC). Executive Order 12382 established the NSTAC, a Presidentially-appointed private sector advisory group, to advise the President on telecommunications matters related to national security/emergency preparedness. OMB, OSTP, and the National Security Council are the NSTAC focal points within the Executive Office of the President, and participate with the Industry Executive Subcommittee in defining the NSTAC agenda.

International Science and Technology Cooperation. OSTP fosters inter-governmental cooperation in science and technology, including coordination of international information network development.

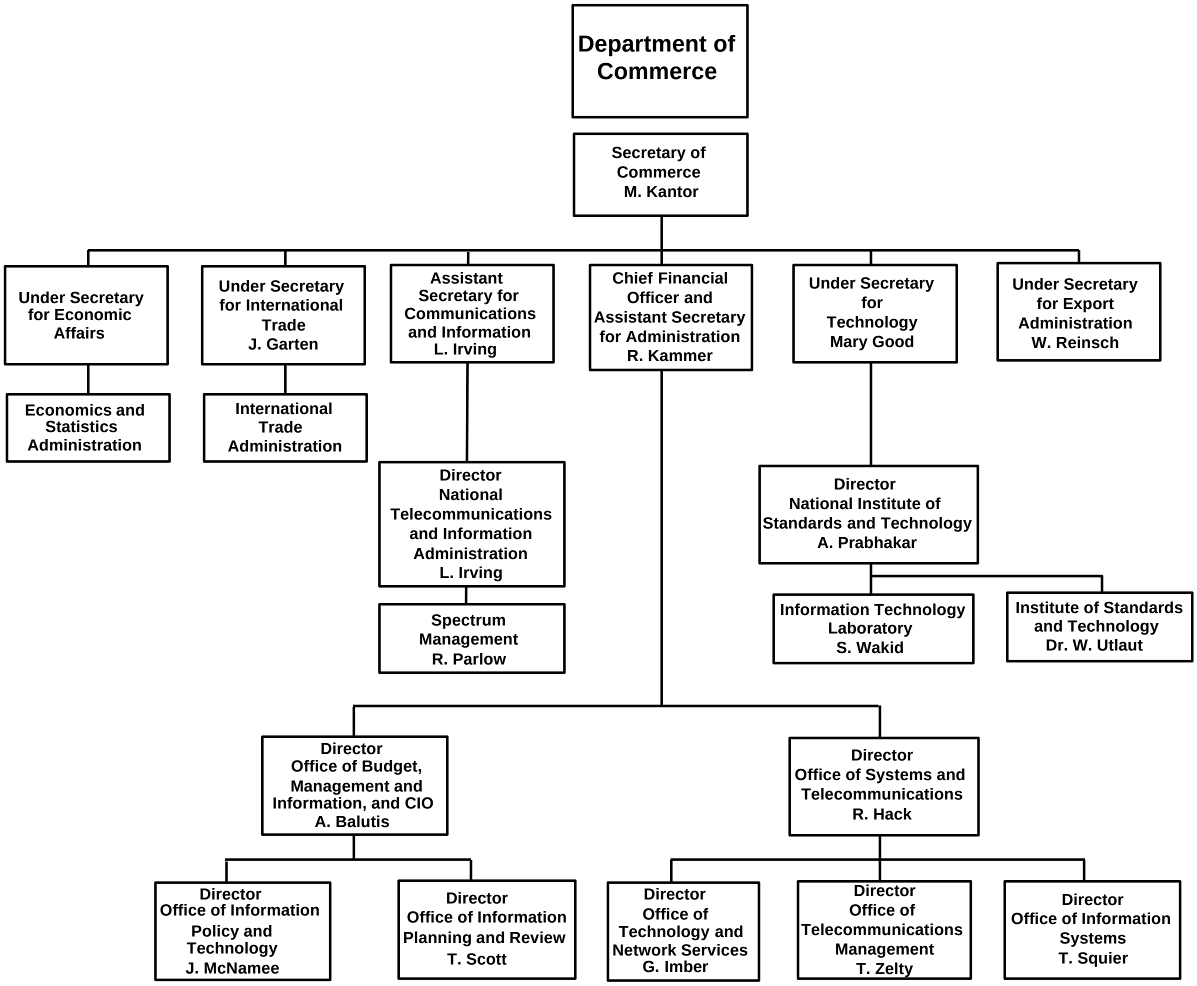
Linkage with the States. The State-Federal Technology Partnership Task Force, which was established by a Presidential directive and is supported by OSTP, seeks to engage federal and state governments in a formal process to represent States at the highest national policy level on science and technology issues. In addition, OSTP has important links with State and regional emergency preparedness activities related to the information infrastructure through association with the National Communications System and the Federal Emergency Management Agency.

Technical Expertise. The technical and policy expertise resident at OSTP includes information networks, computers, and communications systems, and emergency telecommunications services. OSTP also maintains professional relationships with the broader national scientific and technical community.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- OSTP is actively involved in all National Information Infrastructure Task Force activities to include fostering the development of the Global Information Infrastructure.
- A white paper entitled “Towards an Analytical Framework for Infrastructure Protection Policy” describes an analytical approach to assessing the technical aspects of network-related infrastructure vulnerabilities.

This page intentionally left blank.


Department of Commerce
Secretary of Commerce M. Kantor
Under Secretary for Economic Affairs
Economics and Statistics Administration
Under Secretary for International Trade J. Garten
International Trade Administration
Assistant Secretary for Communications and Information L. Irving
Director National Telecommunications and Information Administration L. Irving
Spectrum Management R. Parlow
Chief Financial Officer and Assistant Secretary for Administration R. Kammer
Director Office of Budget, Management and Information, and CIO A. Balutis
Director Office of Information Policy and Technology J. McNamee
Director Office of Information Planning and Review T. Scott
Director Office of Systems and Telecommunications R. Hack
Director Office of Technology and Network Services G. Imber
Director Office of Telecommunications Management T. Zelty
Director Office of Information Systems T. Squier
Under Secretary for Technology Mary Good
Director National Institute of Standards and Technology A. Prabhakar
Information Technology Laboratory S. Wakid
Institute of Standards and Technology Dr. W. Utlaut
Under Secretary for Export Administration W. Reinsch

Organization: Department of Commerce (DoC)

Senior Information Assurance Official:

Raymond Kammer, Chief Financial Officer and Assistant Secretary for Administration

Information Assurance Points of Contact:

Alan Balutis, Director, Office of Budget, Management, and Information
R. Hack, Director, Office of Systems and Telecommunications
G. Imber, Director Office of Technical Support and Network Services
Tom Scott, Director, Office of Information Planning and Review
J. Squier, Director, Office of Information Systems
Tom Zetty, Director, Office of Telecommunications Management

On-Line Resources:

DoC Homepage: http://www.doc.gov

Information Assurance Related Missions and Functions:

The Department of Commerce encourages, serves, and promotes the Nation's international trade, economic growth, and technological advancement. It offers assistance and information to increase America's competitiveness in the world economy; administers programs to prevent unfair foreign trade competition; provides social and economic statistics and analyses for business and government planners; provides research and support for the increased use of scientific, engineering, and technological development; grants patents and registers trademarks; develops policies and conducts research on telecommunications; and provides assistance to promote domestic economic development. It carries out these responsibilities in the Office of the Secretary and its operating units, a selected number of which are described below.

The Bureau of Export Administration is responsible for directing the Nation's export control policy in accordance with the Export Administration Act and the Export Administration Regulations. The Bureau maintains a Commerce Control List of sensitive or dual-use items including software and scientific and technical data which is maintained for national security purposes, to prevent the items from reaching proscribed countries, and for various foreign policy objectives. It exercises control by processing export license applications, conducting foreign availability studies to determine when products should be decontrolled, and enforcing U.S. export control laws.

The International Trade Administration is responsible for promoting world trade and for strengthening the international trade and investment position of the United States. The Bureau of Export Administration and the International Trade Administration were created by law to be separate organizational entities within the Department. In addition to directing the

International Trade Administration, the Under Secretary for International Trade also supervises the U.S. and Foreign Commercial Service. The USFCS develops, produces, markets, and manages an effective line of high-quality products and services geared to the marketing information needs of the U.S. exporting and international business community and manages the delivery of Administration programs through 47 domestic offices and U.S. export assistance centers located in the United States and 132 posts located in 68 countries throughout the world.

The National Oceanic and Atmospheric Administration mission is to explore, map, and chart the global ocean, to describe, monitor, and predict conditions in the atmosphere, ocean, Sun, and space environment, to issue warnings against impending destructive natural events, and to disseminate long-term environmental information. Its principal field organizations include the National Weather Service, the National Marine Fisheries Service, the National Environmental Satellite, Data, and Information Service, the National Ocean Service, and the Office of Oceanic and Atmospheric Research.

The National Telecommunications and Information Administration responsibilities are described in a separate organizational summary.

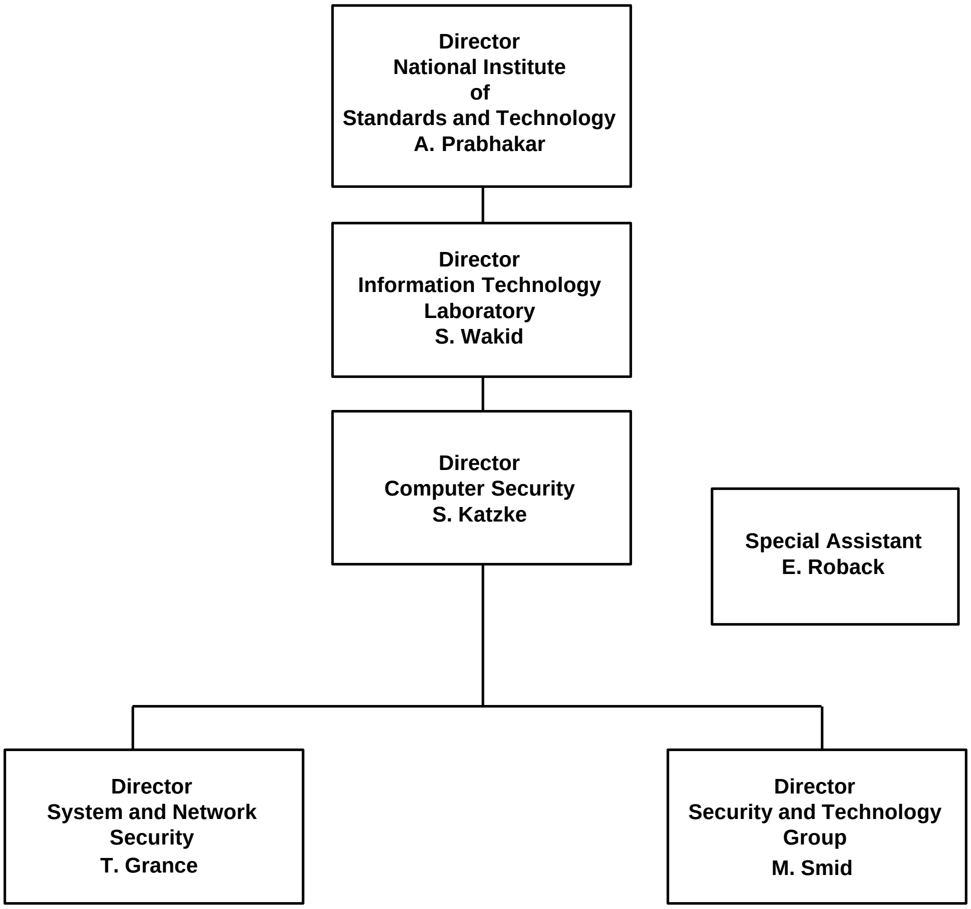
The Technology Administration is responsible for working with U.S. industry in addressing competitiveness issues. It discharges this role through the Office of Technology Policy by advocating coherent policies for maximizing the impact of technology on economic growth, through the National Institute for Standards and Technology (NIST) by carrying out technology programs with U.S. industry, and through the National Technical Information Service by disseminating technology information. Specific National Institute for Standards and Technology responsibilities are described in a separate organizational summary.

The Under Secretary of Commerce advises the Secretary and other Government officials on matters relating to economic developments and forecasts and on the development of macroeconomic and microeconomic policy. The Under Secretary, as the Administrator of the Economics and Statistics Administration, exercises general supervision over the Bureau of the Census and the Bureau of Economic Analysis. The Bureau of the Census collects, tabulates and published a wide variety of statistical data about the people ant the economy of the Nation. The goal of the Bureau of Economic Analysis is to provide a clear picture of the U.S. economy through the preparation, development, and interpretation of the national income and product accounts, summarized by numerous indicators such as the gross domestic product, input-output accounts, etc.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- Standards developed by NIST are released by the Department of Commerce. The Department of Commerce and GSA publish Federal Information Processing Standards.
- Like many other Departments, Commerce is becoming smaller. Ten thousand positions have been eliminated in the last four years; 500 within the last 60 days. The Commerce budget will probably decrease ten to twenty percent in the next fiscal year.

This page intentionally left blank.


Director
National Institute
of
Standards and Technology
A. Prabhakar
Director
Information Technology
Laboratory
S. Wakid
Director
Computer Security
S. Katzke
Special Assistant
E. Roback
Director
System and Network
Security
T. Grance
Director
Security and Technology
Group
M. Smid

Organization: National Institute of Standards and Technology (NIST)

Senior Information Assurance Official:

Shukri Wakid, Director, Information Technology Laboratory

Information Assurance Points of Contact:

Stuart Katzke, Chief, Computer Security Division
Edward Roback, Computer Specialist, Computer Security Division
Tim Grance, Director, Systems and Network Security
M. Smid, Director, Security Technology Group

On-Line Resources:

NIST Homepage: http://www.nist.gov
NIST Security Activities: http://csrc.ncsl.nist.gov/

Information Assurance Related Missions and Functions:

NIST's primary mission is to promote U.S. economic growth by working with industry to develop and apply technology, measurements, and standards. It does this by assisting industry to develop technology to improve product quality, to modernize the manufacturing process, to ensure product reliability, and to facilitate rapid commercialization of products based on new scientific discoveries.

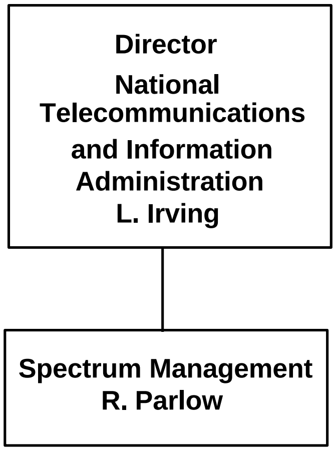
By the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987, NIST was assigned responsibilities to develop government-wide computer system security standards and guidelines and security training programs for the protection of sensitive unclassified information maintained in Federal government computer systems. NIST also administers the Computer System Security and Privacy Advisory Board to advise the Secretary of Commerce and the Director of NIST. The Board also identifies emerging computer security issues and informs the Director, Office of Management and Budget, the Director, National Security Agency, the House Committee on Government Operations, and the Senate Committee on Governmental Affairs of security issues. These responsibilities are carried out by the Information Technology Laboratory (ITL).

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- NIST has approximately 35 people and a base budget of $3.0 million augmented by approximately $3.5 million in other agency funding to fulfill the above responsibilities.
- Significant accomplishments include Data Encryption Standard, Digital Signature Standard, Federal Information Processing Standard (FIPS) 186.

- Debate leading to Computer Security Act of 1987 provides very useful historical perspective. Suggested review of House Government Operations and House Science and Technology Committee reports regarding the legislation.
- Must identify some incremental approach which has cost realism. Policy issues for the private sector must be translated into cost.
- NIST administers the Computer System Security and Privacy Advisory Board which was created by Computer Security Act of 1987. Board consists of volunteers. In general, board is not resourced to properly do its job. Its impact to date has been minimal. The Board’s membership and activities are outlined in a separate organizational summary.
- Many of the recommendations made in the NRC report “Computers at Risk” are still valid. Example is recommendation to establish Information Security Foundation.
- The Interagency Working Group on Cryptographic Policy is chaired by Bruce McConnell of the Office of Management and Budget and Ed Appel of the National Security Council Staff. It includes membership from NIST, NSA, *DoC*, DoJ, FBI, DoS, CIA, Treasury, and others.
- Government Information Technology Service group IT-10 recommended that NIST develop Generally-Accepted Systems Security Practices (GSSP). Stu Katzke is involved in the effort. Expect to publish by mid-1996.
- Information Systems Security Association is also involved in publication of their own GSSP.
- NIST co-chairs the Federal Computer Security Program Manager’s Forum which is described in a separate organizational summary.
- NIST is developing an ITL testing center with special emphasis on security.
- NIST is one of the co-founders of the Forum of Incident Response and Security Teams and until recently provide secretariat services for FIRST.
- NIST acts as resource clearing house for computer security matters and has recently published a computer security handbook
- Pending legal review and approval, NIST will establish a computer emergency response capability to aid Federal departments and agencies in satisfying the recent mandate (Revised Appendix III to OMB Circular A-130) for a such a capability. This capability will be provided on a cost-reimbursable basis using the Department of Energy’s Computer Incident Advisory Capability and the Software Engineering Institute’s Computer Emergency Response Team.
- In June 1996, NIST co-sponsored a conference on vulnerabilities with the intent of developing a modest pilot mechanism for sharing vulnerability information. Other sponsors included DARPA, NCS, and COAST.

This page intentionally left blank.



Director

National Telecommunications and Information Administration

L. Irving

Spectrum Management

R. Parlow

Organization: National Telecommunications Information Administration (NTIA)

Senior Information Assurance Official:

Larry Irving, Administrator

Information Assurance Points of Contact:

Dick Parlow, Chief, Office of Spectrum Management
Bill Gamble, Office of Spectrum Management

On-Line Resources:

NTIA Homepage: http://www.ntia.doc.gov

Information Assurance Related Missions and Functions:

The National Telecommunications and Information Administration responsibilities are to serve as the principal executive branch advisor to the President on telecommunications and information policy, to develop and present U.S. plans and policies at international communications conferences and related meetings, to coordinate U.S. Government positions on communications with the Federal Communications Commission, the U.S. Department of State, and other Federal agencies, to prescribe policies for and managing Federal use of the radio frequency spectrum, to serve as the principal Federal telecommunications research and engineering laboratory through the Institute for Telecommunications Sciences, to provide grants through the Telecommunications and Information Infrastructure Assistance Program (TIIAP) for planning and demonstration projects to promote the development and widespread availability of advanced telecommunications technologies, to provide grants through the Public Telecommunications Facilities Program to extend delivery of public telecommunications services to U.S. citizens and to strengthen the capabilities of existing public broadcasting stations to provide telecommunications services.

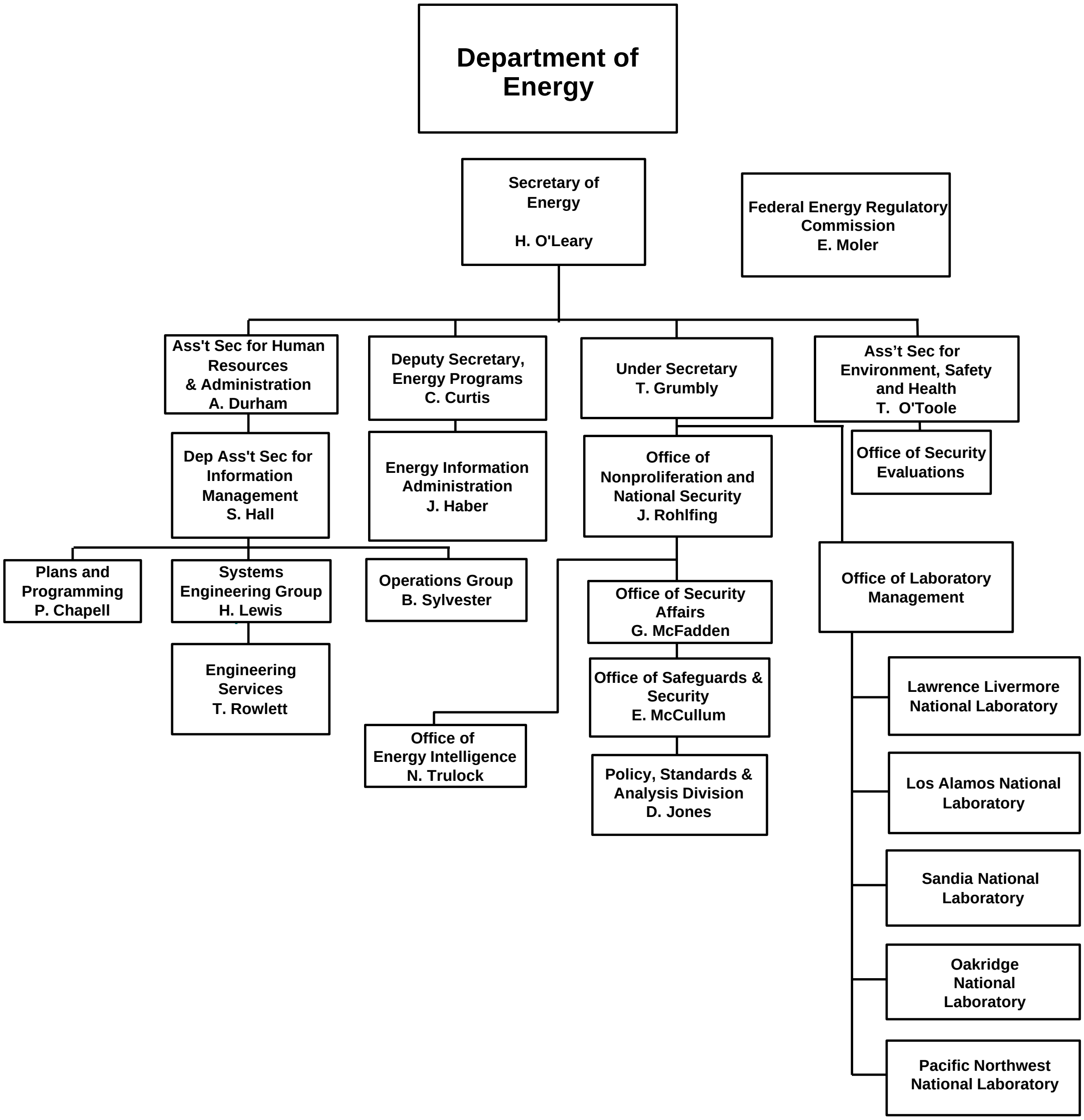
Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- NTIA has been a participant in most Information Infrastructure Task Force committees and working groups. NTIA is actively involved in all wireless activities related to IITF.
- NTIA also participates in bilateral activities related to deregulation, opening markets, etc. Other participants include Office of U.S. Trade Representative, International Trade Administration, and DoS.
- The Institute of Telecommunications Sciences at Boulder, CO, does telecommunications research (e.g., propagation characteristics). ITS also participates in standards development for wireline environment.
- NTIA administers the Telecommunications and Information Infrastructure Assistance Program, a grant program appropriated $21.5M for FY96 by enactment of Public Law 104-134 on April 26, 1996. In all, 809 applications requesting a total amount of $260M

were received from 50 states, the District of Columbia, and the Commonwealth of Puerto Rico.

- NTIA also administers the Public Telecommunications Facilities Program, a grant program appropriated $15.5M for FY96.
- Further information can be obtained from the Director, Public Broadcasting Division, Dennis Connors, Telephone: 202-482-1835, Fax: 202482-2156, E-mail: ptfp@ntia.doc.gov, and from the Acting Director, Telecommunications and Information Infrastructure Assistance Program, Stephen J. Downs, Telephone: 202-482-2048, Fax: 202-501-5136, E-mail: tiiap@ntia.doc.gov.

This page intentionally left blank.


Department of Energy
Secretary of Energy H. O'Leary
Federal Energy Regulatory Commission E. Moler
Ass't Sec for Human Resources & Administration A. Durham
Deputy Secretary, Energy Programs C. Curtis
Under Secretary T. Grumbly
Ass’t Sec for Environment, Safety and Health T. O'Toole
Dep Ass't Sec for Information Management S. Hall
Energy Information Administration J. Haber
Office of Nonproliferation and National Security J. Rohlfing
Office of Security Evaluations
Plans and Programming P. Chapell
Systems Engineering Group H. Lewis
Operations Group B. Sylvester
Office of Security Affairs G. McFadden
Office of Laboratory Management
Engineering Services T. Rowlett
Office of Safeguards & Security E. McCullum
Office of Energy Intelligence N. Trulock
Policy, Standards & Analysis Division D. Jones
Lawrence Livermore National Laboratory
Los Alamos National Laboratory
Sandia National Laboratory
Oakridge National Laboratory
Pacific Northwest National Laboratory

Organization: Department of Energy (DoE)

Senior Information Assurance Official:

Gen. George L. McFadden, Jr., Director, Office of Security Affairs
Spain W. Hall, Jr., Deputy Assistant Secretary for Information Management

Information Assurance Points of Contact:

Larry Wilcher, Program Manager, Information Assurance Program
Tom Rowlett, Director, Engineering Services, Systems Engineering Group,
Information Resources Management
Brent Frampton, Computer Security Specialist, Energy Information Administration
Mary Beth Davis, Deputy Director, Office of Energy Intelligence

On-Line Resources:

DoE Homepage: http://www.ntia.doc.gov/

Information Assurance Related Missions and Functions:

The Department of Energy provides the framework for a comprehensive and balanced national energy plan throughout the coordination and administration of the energy functions of the Federal government. The Department is also responsible for energy regulatory programs and a central energy data collection and analysis programs.

The Office of Non Proliferation and National Security safeguards and secures classified information and protects Departmental and Department of Energy contractor facilities, National Laboratories and installations, manages the Department's Emergency Management System, which responds to and mitigates the consequences resulting from operational, energy, and continuity of Government emergencies.

The Office of Energy Intelligence detects and defeats foreign intelligence services bent on acquiring sensitive information on the Department's programs, facilities, technology, and personnel.

The Office of Information Resources Management is responsible for development and implementation of policy regarding the protection of sensitive but unclassified information.

The Office of the Assistant Secretary for Environment, Safety, and Health is responsible for independent oversight of nuclear/non-nuclear safety and security laws, regulations, and policies.

The Energy Information Administration is responsible of the timely and accurate collection, processing, and publication of data in the areas of energy resource reserves, energy production, demand, consumption, distribution and technology.

The Federal Energy Regulatory Commission is responsible for setting rates and charges for the transportation and sale of natural gas and for the transmission and sale of electricity and the licensing of hydroelectric power projects.

The Office of Laboratory Management is responsible for institutional policy and oversight functions related to utilization of the Department of Energy's multiprogram laboratories to assure optimum utilization of the Department's laboratory complex for meeting national research and technology development objectives. Organizational summaries for the Lawrence Livermore National Laboratory, the Los Alamos National Laboratory, Sandia National Laboratories, Oak Ridge National Laboratory, and Pacific Northwest National Laboratory follow.

Information Assurance Activities, Issues, Best Practices, Lessons Learned: (Rewrite)

- Information security responsibilities split in DoE. Office of IRM responsible for unclassified information (to include connections to Internet). Office of Nonproliferation and National Security responsible for classified information. Office of Energy Intelligence.
- Office of IRM currently working on a DoE policy for sensitive unclassified information with primary emphasis on encypherment.
- The Assistant Secretary for Environment, Safety, and Health operates an Office of Security Evaluations.
- DOE's ESNet is primary backbone of Internet.
- Office of IRM's Engineering Services and the Office of Safeguards and Security sponsor the Computer Incident Advisory Capability (CIAC) operated by the Lawrence Livermore National Laboratory. CIAC also provides information security assistance visits as requested.
- Must emphasize responsibilities of information owners and hold them accountable.
- Moving away from specific policy directives to guidance.
- DoE owns National Laboratory facilities and products of research. Laboratories are operated by independent entities, such as the University of California.
- Current DoE information assurance issues:
  - Finding a cohesive and structured approach to a graded system of information protection from unclassified up through the highest levels of classified.
  - DoE Information Assurance Infrastructure.
  - Efforts to identify DoE key assets.
  - There is a lack of funding for security initiatives.

Organization: Lawrence Livermore National Laboratory (LLNL)

Senior Information Assurance Official:

David M. Cooper, Associate Director for Computation

Information Assurance Points of Contact:

Doug L. Mansur, Head, Computer Security Technology Center

On-Line Resources:

LLNL Homepage: http://www.llnl.gov
Computer Incident Advisory Capability: http://ciac.llnl.gov/ciac/notes/

Information Assurance Related Missions and Functions:

The Computer Security Technology Center (CSTC) is an element of the Computation Organization at the LLNL; it serves the needs of clients in the U.S. Department of Energy (DoE) and other federal agencies. The CSTC delivers solutions to today's information technology security challenges through integration of operations; incident response, product development, and consulting services.

Computer Incident Advisory Capability (CIAC) is an element of the CSTC and is also located at LLNL. CIAC provides computer security free of charge to employees and contractors of the DoE; these services include: incident handling, computer security information, on-site workshops, and computer security consulting. CIAC provides operational incident response and serves as the single point of contact for all DoE incident handling. This team gathers fast-breaking vulnerability and threat information and disseminates it throughout the DoE community. CIAC is also a founding member of Forum of Incident Response and Security Teams (FIRST).

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Lawrence Livermore National Laboratory is engaged in a joint effort with the Los Alamos National Laboratory and the Sandia National Laboratories to develop a real-time intrusion detection and response system that can supplement or complement an information assurance program for protecting the Department's information resources.
- Other Information Assurance activities emphasize network security topics, with particular specialization in the areas of network security alarms, vulnerability analyses and profiles, network intrusion detection, security profiles, firewall architecture, education, and tools for security management

Organization: Los Alamos National Laboratory (LANL)

Senior Information Assurance Official:

Debra Rutherford, Program Manager, Safeguards & Security

Information Assurance Points of Contact:

William J. Hunteman, Project Leader, Information Assurance

On-Line Resources:

LANL Homepage: http://www.lanl.gov:8010/

Information Assurance Related Missions and Functions:

The computer networks of the LANL are divided into two parts. One part contains the nuclear weapons information and has no connection to the outside world. It cannot be accessed by anyone from outside the laboratory.

The Computer Research and Applications Group builds fraud detection software for many special purpose projects. Most of the group's research tends to be with on-line training and operating modes, adaptive systems, and neural net type systems.

The Network Anomaly Detection Intrusion Reporter (NADIR) system has been running on the laboratory's network since 1989. The goals of this system are detection, deterrence, and accountability. It is an expert system-an automated audit system. The network, all the nodes attached to it, and all the computers have always had the requirements for forming logs and reporting. NADIR has now taken over the task of looking through these logs and detecting anomalous behavior.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Los Alamos National Laboratory is engaged in a joint effort with the Lawrence Livermore National Laboratory and the Sandia National Laboratory to develop a real-time intrusion detection and response system that can supplement or complement an information assurance program for protecting the Department's information resources.
- The Los Alamos National Laboratory is heavily engaged in short-term on-site support for Departmental entities. This support emphasizes response to unique or critical requirements, or those which involve specialized expertise. Support may include conducting assessments or providing security advice and assistance in all phases of system design, development, and implementation.

Organization: Oak Ridge National Laboratory (ORNL)

Senior Information Assurance Official:

George A. Dailey, Director, Data Systems Research and Development Program

Information Assurance Points of Contact:

Sharon Jacobsen, Manager, Communications and Security Department

On-Line Resources:

ORNL Homepage: http://www.ORNL.gov

Information Assurance Related Missions and Functions:

The Data Systems Research and Development (DSRD) Department of Energy (DoE) Center for Information Security Technology (CIST) was established in 1986 as a joint sponsorship by the Department of Energy and the Department of State. CIST provides support at the national level for a variety of federal agencies, as well as for the Department of Energy and Lockheed Martin Energy Systems. The CIST mission is to provide research, development, demonstration, and application testing and evaluation of information security technologies focusing on the assessment of technologies for use in the classified and unclassified sensitive sectors.

A staff of information security professionals with state-of-the-art technology resources focuses on the protection of classified and unclassified systems for processing information up to and including Top Secret. The experience gained from information management applications that include major accounting and financial transactions, command and control, law enforcement, and many other diverse areas of government concern is available to all CIST activities.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Oak Ridge National Laboratories are responsible for developing and delivering training and education in all areas of DOE Automated Information System Security. Subject matter ranges from regulatory to technical, and is targeted at all personnel involved with information systems security including managers, information system security professionals, and system users. Additional activity is devoted to secure distributed databases, developing a Multilevel Secure (MLS) Local Area Network, and developing an MLS document storage and retrieval system.

Organization: Pacific Northwest National Laboratory (PNNL)

Senior Information Assurance Official:

Thomas R. Fox, Associate Laboratory Director, National Security Division

Information Assurance Points of Contact:

D. R. Miles, Staff Scientist, DOE Information Security Resource Center

On-Line Resources:

PNNL Homepage: http://www.pnl.gov

Information Assurance Related Missions and Functions:

The Information Security Resource Center (ISRC) collects, analyzes, and disseminates information germane to the Department's Information Assurance activities. Sources include public networks, telecommunication industry sources, Government Agencies, and the Department Contractor Complex. Open source information regarding subjects relating to the protection and integrity of the Department's sensitive information is also collected and analyzed. Information acquisition and analysis is also intended to support policy development.

Information of interest includes that related to protecting information, information systems, and key information resource assets (e.g., telephone systems, power systems, networks). Emphasis is placed on acquisition of information which facilitates development of layered, risk-management-based defenses to guard against attacks on information resources and information assets. Other functions include coordinating protection of information and key information resource assets and ensuring coordination of programmatic and Information Assurance managers.

Information Assurance Activities, Best Practices, Lessons Learned:

- The Pacific Northwest National Laboratories are developing and implementing a database for threat information, and designing and evaluating advanced concepts for data retrieval and analysis. Current initiatives include development of visualization methodologies, technologies, and tools for application to databases which are characterized by having large quantities of data in which the information content is obscured or not readily identifiable by traditional means.

Organization: Sandia National Laboratory (SNL)

Senior Information Assurance Official:

Samuel G. Varnado, Director, Information Systems Engineering Center

Information Assurance Points of Contact:

Patricia C. Sprauer, Program Manager, Information Assurance Research and Development

On-Line Resources:

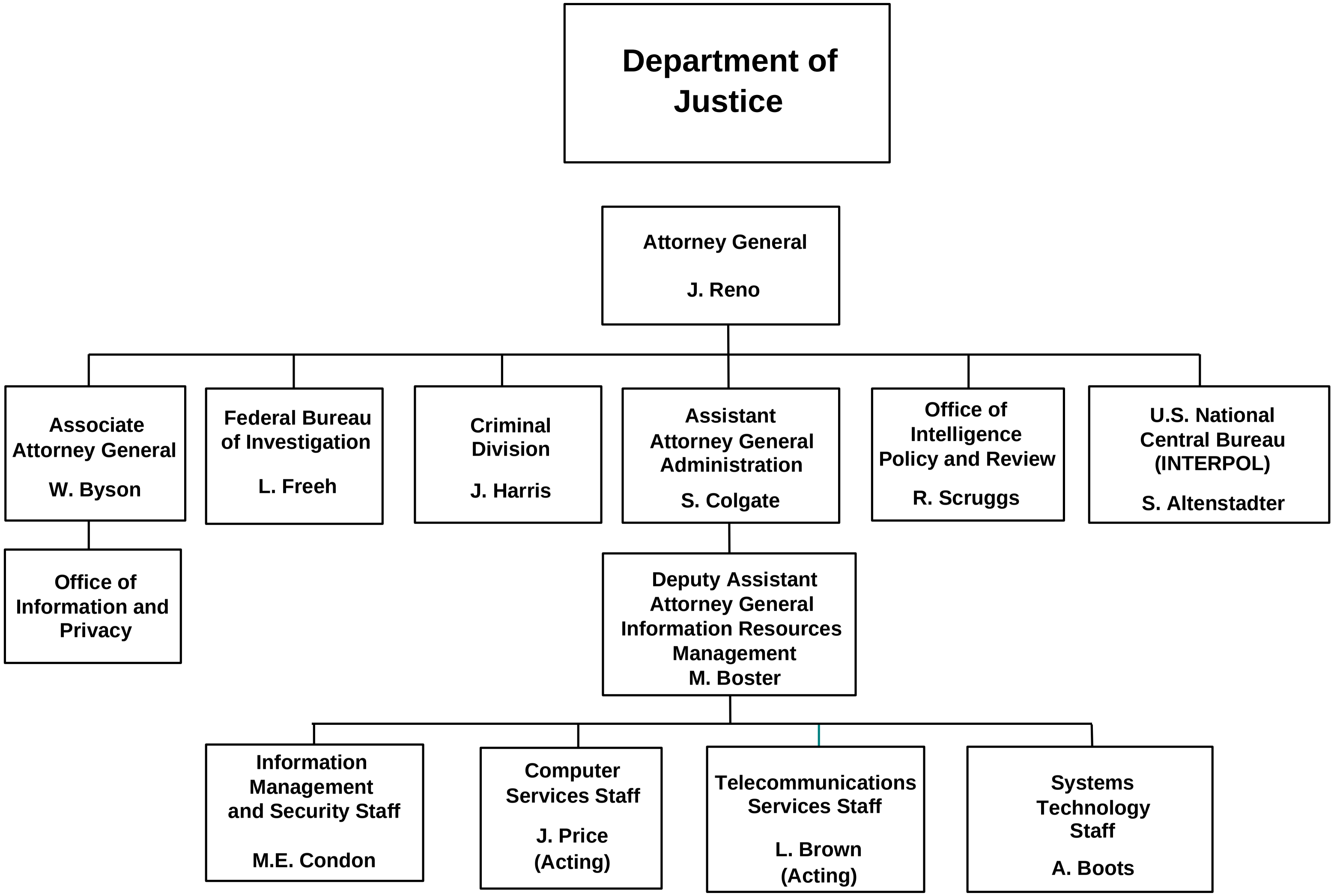
SNL Homepage: http://www.sandia.gov/

Information Assurance Related Missions and Functions:

The end of the Cold War era has stimulated DOE's national laboratories to contribute to economic security, synergistic with their public missions in defense, energy, and the environment. Recognizing the complexity of the issues and relationships for industry-led and government partnered enterprises, Sandia's National Industrial Alliances Center has developed and implemented the Prosperity Games in partnership with the National War College, Lawrence Livermore National Laboratories, the Electronics Industries Association, and the American Electronics Association. Under the auspices of the Electronics Subcommittee of the NSTC, the Prosperity Games have provided energy for and assessment of road maps of the technology and policy options related to electronic manufacturing in the United States.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Sandia National Laboratories are engaged in a joint effort with the Los Alamos National Laboratory and the Lawrence Livermore National Laboratory to develop a real-time intrusion detection and response system that can supplement or complement an information assurance program for protecting the Department's information resources.
- The Sandia National Laboratories are also heavily involved in a broad range of authentication and encryption topical areas in addition to information surety, firewall architecture, data base design and implementation, and educational delivery methodologies and mechanisms.


Department of Justice
Attorney General
J. Reno
Associate Attorney General
W. Byson
Federal Bureau of Investigation
L. Freeh
Criminal Division
J. Harris
Assistant Attorney General Administration
S. Colgate
Office of Intelligence Policy and Review
R. Scruggs
U.S. National Central Bureau (INTERPOL)
S. Altenstadter
Office of Information and Privacy
Deputy Assistant Attorney General Information Resources Management
M. Boster
Information Management and Security Staff
M.E. Condon
Computer Services Staff
J. Price (Acting)
Telecommunications Services Staff
L. Brown (Acting)
Systems Technology Staff
A. Boots

Organization: Department of Justice (DoJ)

Senior Information Assurance Official:

Stephen R. Colgate, Assistant Attorney General For Administration

Information Assurance Points of Contact:

Mark A. Boster, Deputy Assistant Attorney General for Information Resources Management (IRM)
Mary Ellen Condon, Director, Information Management and Security Staff (IMSS), IRM
Scott Charney, Chief, Computer Crime Unit, Criminal Division
Robert Bryant, Assistant Director, National Security Division, FBI
Neil J. Gallagher, Deputy Assistant Director, Criminal Investigative Division, FBI

On-Line Resources:

DoJ Homepage:	http://www.usdoj.gov/
Federal Bureau of Investigation:	http://www.fbi.gov/
FBI National Computer Crime Squad:	http://www.fbi.gov/compcrim.htm
Drug Enforcement Agency:	http://www.usdoj.gov/dea/deahome.htm

Information Assurance Related Missions and Functions:

The Department of Justice serves as counsel for the Nation's citizens. It exercises this primary responsibility through law enforcement, crime prevention, crime detection, prosecution, incarceration, and rehabilitation of offenders.

The Office of Information and Privacy coordinates policy development and Government-wide compliance with the Freedom of Information and Privacy Acts.

The Justice Management Division (JMD) provides assistance to senior management officials concerning basic departmental policy for automatic data processing, telecommunications, security, and records management, as well as budget and financial management, personnel management and training, equal opportunity programs, procurement, real property and materiel management, and for all other matters pertaining to organization, management and administration. JMD develops and disseminates policies, standards and procedures for managing automated information processing resources. JMD also reviews the implementation of these policies, standards and procedures. In addition, JMD provides automated litigation support, and collects, organizes, and disseminates recorded information that is necessary to the DoJ in carrying out its statutory mandates.

The Office of Intelligence Policy and Review advises the Attorney General on national security matters. The office prepares and files applications for surveillance under the Foreign Intelligence Surveillance Act of 1978 and advises all Government agencies on national security law.

The Antitrust Division is responsible for promoting and maintaining competitive markets by enforcing the Federal antitrust statutes and by acting as an advocate of competition within the Federal government. The division also represents the United States in judicial proceedings to review certain orders of regulatory bodies such as the Federal Communications Commission.

The Criminal Division develops, enforces and supervises the application of all Federal criminal statutes, except those specifically assigned to other divisions. The division includes the Fraud Section that directs and coordinates the Federal effort against fraud and white collar crime; the Internal Security Section that supervises the investigation and prosecution of cases affecting the national security, foreign relations, and the export of military and strategic commodities and technology; and the Money Laundering Section. Also included it the Computer Crime Unit, which is responsible for implementing the Computer Crime Initiative, a five-point program that is designed to respond to the mounting computer crime problem.

DoJ takes a keen interest in investigating and prosecuting computer crimes ranging from intrusions prosecuted under Title 18 USC § 1030 to communication of threats over networks. DoJ is interested not only in crimes directed against DoJ facilities but in all violations of Federal law. for example, DoJ works closely with the Air Force’s Office of Special Investigations and other military components to address attacks against military computer systems.

The Federal Bureau of Investigation is the principal investigative arm of the Department. At present, organized crime/drugs, counterterrorism, white collar crime, foreign counterintelligence, and violent crime are the Bureau’s investigative priorities. The Economic Crime Unit in the White Collar Crime Section of the Criminal Investigative Division has primary responsibility for computer crime investigations.

The United States National Central Bureau represents the United States in the International Criminal Police Organization (INTERPOL). The National Central Bureau provides an essential communications link between the U.S. police community and their counterparts in foreign member countries.

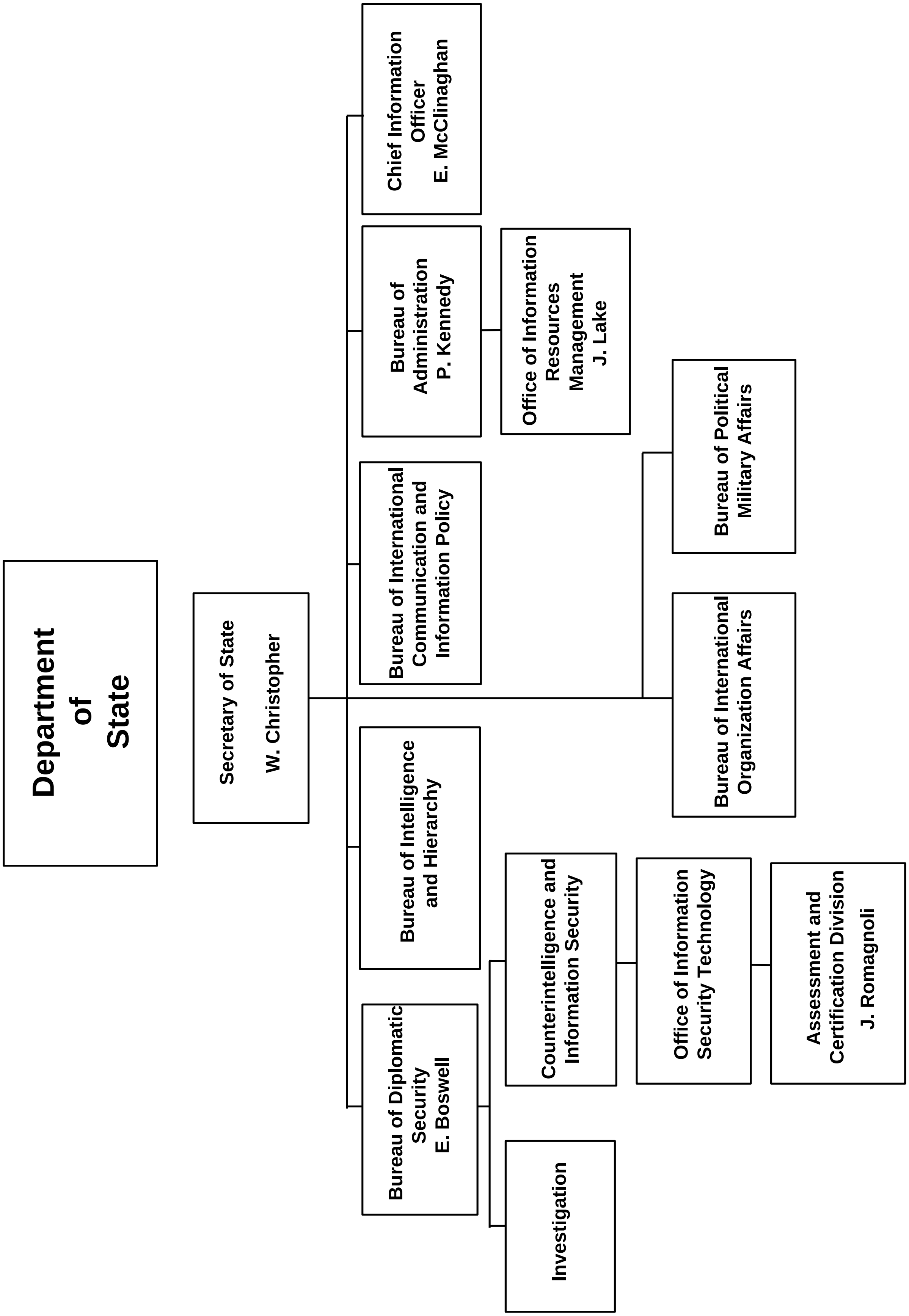
Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Department has formed a Computer Security Officers Task Force consisting of the representatives with computer security responsibility from each of the Departments 34 components. Each component Computer Systems Program Manager is responsible for overseeing the activities of Computer Systems Security Officers designated for each system. These systems security officers are full-time or part-time security specialists, depending on the size and sensitivity of the system and its information.
- The Department has unique information protection requirements. On one hand it is obligated to share its information with the public and other law enforcement agencies. On the other, the information held at the Department, such as evidence and fingerprints, is very sensitive information. In addition, DoJ must share considerable information with the Judiciary.
- Since DoJ is the principal agency responsible for the Federal government's litigation and law enforcement functions, many critical systems and services could be affected: immigration and border controls; criminal investigations; civil suits, many involving large sums of money; control of the Federal prison system; litigation and settlements in antitrust cases; litigation of criminal and civil tax cases; matters involving environmental laws; and many others. Specifically in the area of national security, the Department handles many sensitive matters involving intelligence information, including wiretaps under the Foreign Intelligence Surveillance Act; FBI counterintelligence investigation; and liaison operations of the FBI, Drug Enforcement Agency and others in foreign countries.
- DoJ is in the midst of proposing legislation to further strengthen the laws available to prosecutors in the high-technology area (Title 18 U.S.C. § amendments, copyright provisions, Privacy Protection Act, etc.).
- The Criminal Division coordinates closely with many other components, such as the FBI National Computer Crime Squad and the FBI Computer Analysis and Response Team, to exchange information and develop better legal and tactical approaches to computer crimes. DoJ also coordinates with the Secret Service, IRS, Air Force, Navy, and others.
- Each U.S. Attorney's Office designates a Computer/Telecommunications Coordinator. These coordinators are prosecutors who receive special training in technology issues to act as the central point of contact who understands technical matters.
- Information protection is accomplished by risk management, which includes estimates of the viability of the threat and value of the information that must be protected. The threat is a validated threat produced at DoJ. Of note, private detectives and skip tracers (people who located others persons who default on bail, loans, etc.) constitute a significant threat to DoJ information, as do organized crime, drug trafficking, etc. Additional considerations include the distribution of information and the data upon which the information is based and the aggregation of information.
- Two projects represent DoJ best practices in information protection: the Counternarcotics Information Sharing Project and the Joint Automated Booking System. The Counternarcotics Information Sharing Project, sometimes referred to as Drug X, is an information pointer system that was developed in a cooperative manner with two components and was based upon extensive discussions with the users. Developing the system involved developing an architecture based on multiple platforms and information

protection requirements. The Joint Automated Booking System was developed by five DoJ components.

- The Department's Justice Performance Review Office recently received approval to establish a Computer Security Technical Laboratory, which will include a DoJ Incident Response Service (DOJIRS) and an advanced authentication and encryption test bed.
- Information security policy oversight for unclassified DoJ systems is conducted by the IMSS. The basis for policy is the existing body of laws and regulations regarding matters with which the various components of DoJ must deal. IMSS relies on the DoJ components to provide legal advice and assistance. The staff translates the laws and regulations into technical policy which is then disseminated to the components. components also write implementing policy which the IMSS periodically reviews for compliance with higher level policy. The policy is also based on existing Executive Branch policy and standards to include NIST standards where applicable. In general, existing technical policy is centered on the goal of C2 level of protection of information. Implementation of the policy is also complicated by legacy systems and rapid changes in technology.
- There are now four staffs instead of five under the Deputy Assistant Attorney General for IRM, Mark A. Boster. The Computer and Telecommunications Security Staff (CTSS) and the Systems Policy Staff were combined to form the Information Management and Security Staff (IMSS), headed by Mary Ellen Condon. IMSS has responsibility for all the policy and security functions that were handled by CTSS in the past.
- The FBI is expanding its outreach program to industry, known as Development of Espionage, Counterintelligence and Counterterrorism Awareness (DECA) program, to include a communications network to inform corporations of industrial spying and technology transfer threats and to provide defensive tips. The Bureau plans to include computer crimes against industry in the information to be addressed.
- The FBI and the Secret Service have formed a coordination group with several banking associations to combat financial fraud and computer crimes. The banking associations include the Washington-based American Bankers Association, Independent Bankers of America, America's Community Bankers, and the Credit Union National Association. [Washington Technology, May 23, 1996, page 8]

This page intentionally left blank.


Department of State
Secretary of State
W. Christopher
Chief Information Officer
E. McClinaghan
Bureau of Administration
P. Kennedy
Office of Information Resources Management
J. Lake
Bureau of International Communication and Information Policy
Bureau of Political Military Affairs
Bureau of International Organization Affairs
Bureau of Intelligence and Hierarchy
Bureau of Diplomatic Security
E. Boswell
Counterintelligence and Information Security
Office of Information Security Technology
Assessment and Certification Division
J. Romagnoli
Investigation

Organization: Department of State (DoS)

Senior Information Assurance Official:

Eric Boswell, Assistant Secretary for Diplomatic Security

Information Assurance Points of Contact:

Eliza McClenaghan, Chief Information Officer
Joseph Lake, Deputy Assistant Secretary for Information Management
Jules Romagnoli, Chief, Assessment and Certification Division, Bureau of Diplomatic Security

On-Line Resources:

DoS Homepage: http://www.whitehouse.gov/WH/Cabinet/html/Department_of_State.html

Information Assurance Related Missions and Functions:

The Department of State advises the President in the formulation and execution of foreign policy. The Department's primary objective in the conduct of foreign relations is to promote the long-range security and well-being of the United States.

The Secretary is the first ranking member of the Cabinet and a member of the National Security Council. The Under Secretary for International Security Affairs is responsible for assuring the integration of all elements of the Foreign Assistance Program and serves as the Chairman of the Arms Transfer Management Group. The Under Secretary is also responsible for international scientific and technological issues, communications and information issues, and technology transfers.

The Bureau of Diplomatic Security provides a secure environment for conducting American diplomacy and promoting American interests worldwide. It assists the Secretary in the formulation and implementation of diplomatic security policy to provide a secure environment for the conduct of American diplomacy and coordinates the exchange of security-related intelligence and operational information among the Department, foreign governments, other U.S. Government agencies, and all law enforcement authorities. The Bureau provides administrative support to the Overseas Security Advisory Council, a Federal Advisory Committee, which provides for regular and timely exchange of information between the private sector and the Department.

The Bureau of Intelligence and Research coordinates the programs of intelligence, analysis, and research and produced intelligence studies and current intelligence analyses.

The Bureau of International Communications and Information Policy coordinates with other U.S. Government agencies and the private sector in the formulation and implementation of international policies relating to a wide range of rapidly evolving communications and information technologies. The Bureau also promotes U.S. telecommunications interests bilaterally and multilaterally.

The Bureau of International Organization Affairs leads in the development, coordination, and implementation of U.S. multilateral policy. It formulates and implements U.S. policy toward international organizations with particular emphasis on those organizations which make up the United Nations system.

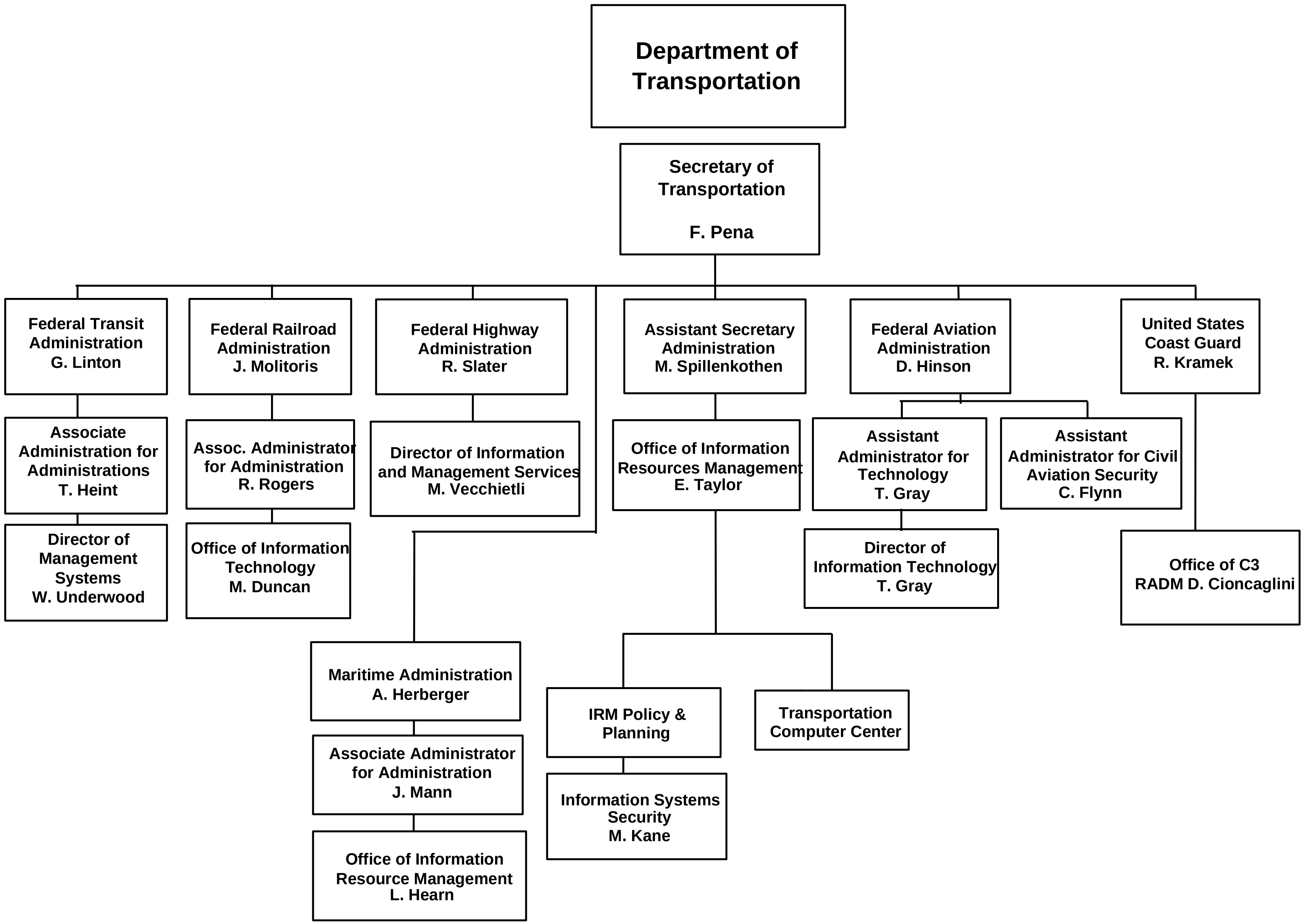
The Bureau of Political-Military Affairs coordinates policy formulation on national security issues including defense relations and security assistance and export controls. The Bureau's major activities are designed to further U.S. national security objectives by through negotiations, security assistance, curbing proliferation of weapons of mass destruction, and inhibiting adversaries access t military significant technologies.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Under Secretary for Management has directed the Assistant Secretaries to take responsibility for security of systems under their direction.
- Bureau of Diplomatic Security develops and promulgates security policy with the involvement of the other DoS bureaus. Office of Information Security Technology drafts the policy. Office includes responsibility for records security (Ms. Mary Stone) which includes damage assessment and classification of information.
- DS/CIS participates in the NSTISSC. The Deputy Assistant Secretary for CIS is the DoS representative to NSTISSC. Chief, Assessment and Certification Division is the DoS representative to the SAIS and the STSS.
- Operational communications matters are responsibility of Office of Information Management in the Bureau of Administration. Although Office of Information Management and OIST are in different bureaus, they work closely to integrate security early in the systems development process.
- Security policies are articulated in Foreign Affairs Manual.
- The Department is beginning to emphasize risk management. Some savings have already been achieved by moving to risk management. Also trying to identify responsibilities for Assistant Secretaries and pin point ownership of information.
- Assurance goals are always mitigated by operational considerations.
- Major issues are how to incorporate security in open systems architectures, multilevel security, logical management architectures, and networks. Another issue is the fast-paced introduction of technology which seems to out pace the introduction of security technologies. Also need a standard mechanism for sharing information.
- DoS will use DoD Defense Messaging System -- saves on development. DoS does not do any research and development.
- DoS does, however, operate a computer security laboratory which is configured as a model embassy. The lab is used to test security policies before implementation. The lab

simulates overseas operations for security certification of systems and software. The lab budget is approximately $1.5 million per year. Computer security laboratory used to test, assess, and evaluate security methods. Firewalls used but limit capabilities. Encryption also used but with associated limitations (commonality of equipment, key distribution, limited access, information constraining).

- OIST's education and awareness training are oriented on operational matters, not mandatory security training issues.
- As a result of a recent *Wall Street Journal* article, DoS representatives expect to be called to testify before the Senate Permanent Subcommittee on Investigations which is holding hearings on computer security.
- OIST recently completed a risk management study on providing Internet access to DoS employees. While the business case for Internet access has not been fully developed, the risks associated with several options (desktop, stand-alone, separate network) to providing the service have been fully identified and briefed to management personnel.
- DoS is developing a response plan for computer emergencies. The plan calls for decentralized implementation and is oriented on intrusions from the Internet and viruses. The plan has not yet been fully exercised.
- DoS develops its own tools and procedures to evaluate its systems and networks. These evaluations are conducted based on network complexity, perceived threats, and system and network improvements.
- The Under Secretary for Management and the Chief Information Officer are very knowledgeable of the security risks and have been very supportive of the security programs. For example, the Under Secretary manages a program in which the Bureaus compete for money to support Bureau initiatives which have department-wide value. Approval of a program initiative is contingent on a security approval by OIST and six percent of the program funds must be devoted to security (requirements definition and implementation). A recently approved program has resulted in the electronic delivery of classified and unclassified telegrams employing a from of multilevel security.
- Budget and staffing for information security have remained stable. Some additional funding (nearly 50%) has been made available this fiscal year because of management interest in security initiatives.
- The Office of Information Management has formed a team to define the DoS information infrastructure. Several foundations (e.g., security, configuration management, training) are being established before the infrastructure is defined in detail. It is envisioned that these foundations will lead to standardization and interoperability.
- OIST personnel are devoting special attention to integrity and availability issues.



Department of Transportation

Secretary of Transportation
F. Pena

Federal Transit Administration
G. Linton

Associate Administration for Administrations
T. Heint

Director of Management Systems
W. Underwood

Federal Railroad Administration
J. Molitoris

Assoc. Administrator for Administration
R. Rogers

Office of Information Technology
M. Duncan

Federal Highway Administration
R. Slater

Director of Information and Management Services
M. Vecchietli

Maritime Administration
A. Herberger

Associate Administrator for Administration
J. Mann

Office of Information Resource Management
L. Hearn

Assistant Secretary Administration
M. Spillenkothen

Office of Information Resources Management
E. Taylor

IRM Policy & Planning

Information Systems Security
M. Kane

Transportation Computer Center

Federal Aviation Administration
D. Hinson

Assistant Administrator for Technology
T. Gray

Director of Information Technology
T. Gray

Assistant Administrator for Civil Aviation Security
C. Flynn

United States Coast Guard
R. Kramek

Office of C3
RADM D. Cioncaglini

Organization: Department of Transportation (DoT)

Senior Information Assurance Official:

Mellisa J. Spillenkothen, Assistant Secretary for Administration

Information Assurance Points of Contact:

Michael Kane, DoT Information Systems Security Officer, Office of Information Resource Management

On-Line Resources:

DoT Homepage: http://www.dot.gov
FAA: http://www.faa.gov
FAA Technical Center: http://www.tc.faa.gov/

Information Assurance Related Missions and Functions:

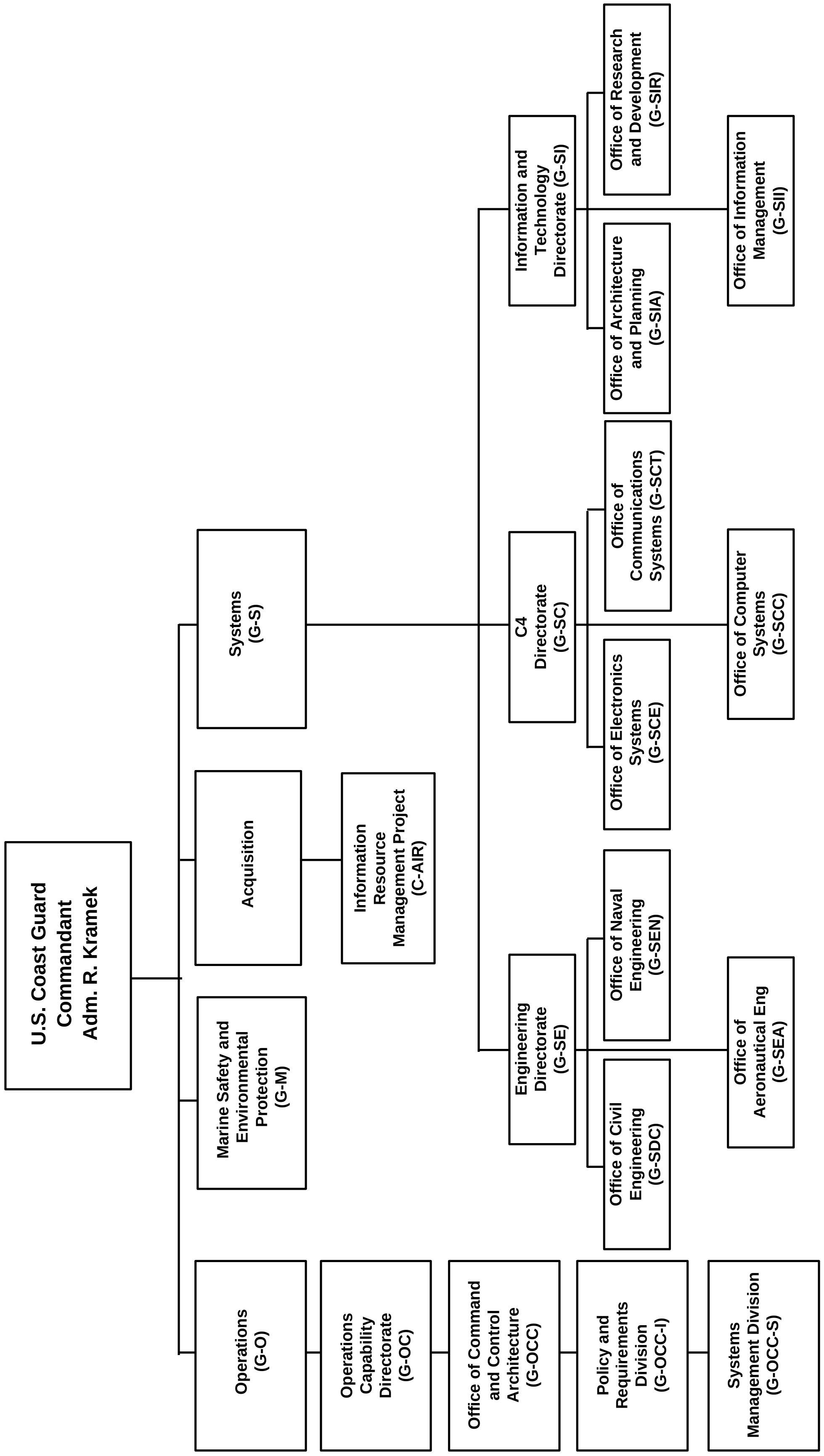
The Office of Information Resource Management formulates, prescribes, and assures compliance with telecommunications and automated data processing policy to include information systems security policy.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Departmental Information Systems Security Officer is supported by a staff of two people. Budget is very limited. U.S. Coast Guard (USCG). has three information security staff personnel supported by nine regional officers who perform information security duties as collateral duties. Federal Aviation Administration (FAA) has two information security staff personnel supported by ten regional officers who perform information security duties as collateral duties. Computer centers (Washington, DC, Plano, TX, Cambridge, MA) have full time security officers.
- Reinvention of DoT may result in:
  - Reduction of operating administrations to three -- FAA, USCG, Intermodal Transportation Agency (ITA)
  - Reduction in employees from 105,000 to 50,000 (Including military)
  - Reduction in grant programs from 30 to 3
  - Privatization of air traffic control activities
- Traditional security concerns in DoT have focused more on keeping planes in the air vice information security.
- Reduction in grant programs will be accompanied by establishment of “Transportation Banks” for disbursement of moneys. This will add enormous security requirements regarding electronic commerce and electronic funds transfer. DOTreas is providing advice on related issues.

- Senior official for information systems security is the Assistant Secretary for Administration, who chairs an Advisory Management Committee (AMC). The Executive Agent for Information Security is Eugene Taylor, the Director of Information Resource Management, who chairs the IRM Advisory Committee (IRMAC). Mr. Kane, the Departmental Information Systems Security Officer, chairs the Subcommittee on Computer Security (SOCS). The AMC and the IRMAC have membership from the operating administrations. The SOCS has membership from the operating administrations, the Inspector General's Office, and the Computer Centers.
- DoT has been actively conducting oversight reviews to improve security posture. Two years ago, only two of ten operating administrations had information security policies. Will actively continue the reviews, some in the form of self assessments.
- Reviews resulted in establishment of a very good training and awareness program which has been very effective at the end-user level. Still need a similar program to influence management. Will address all OPM and procurement categories and establish performance areas for executives, senior functional managers, IRM personnel, and security personnel.
- DoT uses a departmental security banner on all systems. Also employs a user authorization form for every user.
- Growth of electronic commerce may outrun our ability to adequately secure the commerce. Help from GSA (responsible for the security infrastructure) slow in coming.
- DoT has completed extensive policy-to-standards translations.
- Intend to do penetration demonstration for senior managers in near future.
- DoT concerned about whether significant employee reductions will increase insider threat.
- Mr. Kane thinks the Federal Computer Security Program Manager's Forum is productive.
- Information security issues:
  - Multiple e-mail protocols and associated problems.
  - Reinvention of DoT means a new corporate architecture.
  - Which encryption schemes to use (hardware, software, embedded, digital signature standard).
  - Use of conformance standards and how to couple with controls.
- Security must be cost effective and consistent with information being protected. Simple quick-fix, low cost solutions are available.
- Have experienced several penetrations. In one instance, the Intermodal LAN was penetrated within hours of its activation. The perpetrator used the LAN to weave to Maryland and Virginia banks and other sensitive operations.
- The Office of Information Resources Management is in the process of establishing the Information Technology Omnibus Procurement, a multi-year, multiple award contract valued at over $1 billion which will be used to provide information systems engineering, facilities management, and systems security services to the entire department on a fee-for-service basis. It is expected that awards will be made by October 1, 1996.
- The budget for information technology (including information systems security) is shrinking.

This page intentionally left blank.


U.S. Coast Guard Commandant Adm. R. Kramek
Operations (G-O)
Operations Capability Directorate (G-OC)
Office of Command and Control Architecture (G-OCC)
Policy and Requirements Division (G-OCC-I)
Systems Management Division (G-OCC-S)
Marine Safety and Environmental Protection (G-M)
Acquisition
Information Resource Management Project (C-AIR)
Systems (G-S)
Engineering Directorate (G-SE)
Office of Civil Engineering (G-SDC)
Office of Naval Engineering (G-SEN)
Office of Aeronautical Eng (G-SEA)
C4 Directorate (G-SC)
Office of Electronics Systems (G-SCE)
Office of Communications Systems (G-SCT)
Office of Computer Systems (G-SCC)
Information and Technology Directorate (G-SI)
Office of Architecture and Planning (G-SIA)
Office of Research and Development (G-SIR)
Office of Information Management (G-SII)

Organization: United States Coast Guard (USCG)

Senior Information Assurance Official:

RADM John Tozzi, Director, Information and Technology Directorate (G-SI)

Information Assurance Points of Contact:

CAPT Dave Potter, C4 Directorate, Systems
CAPT Dick Mead, Office of Command and Control Architecture, Operations
LCDR Mike Inman, Office of Command and Control Architecture, Operations
CAPT Ben Chiswell, Office of Communications Systems, C4 Directorate, Systems
CDR Mike Grimes, Office of Communications Systems, C4 Directorate, Systems

On-Line Resources:

USCG Homepage: http://www.dot.gov/dotinfo/uscg/

Information Assurance Related Organizations, Missions and Functions:

USCG missions include: Maritime Search and Rescue, Ice Operations and Marine Science Activities, Commercial Vessel Safety, Marine Environmental Protection, Port Safety and Security, Maritime Law Enforcement/Enforcement of Laws and Treaties, Contingency Preparedness/Defense Operations and Recreational Boating Safety. It is subordinate to the Navy during time of national emergency.

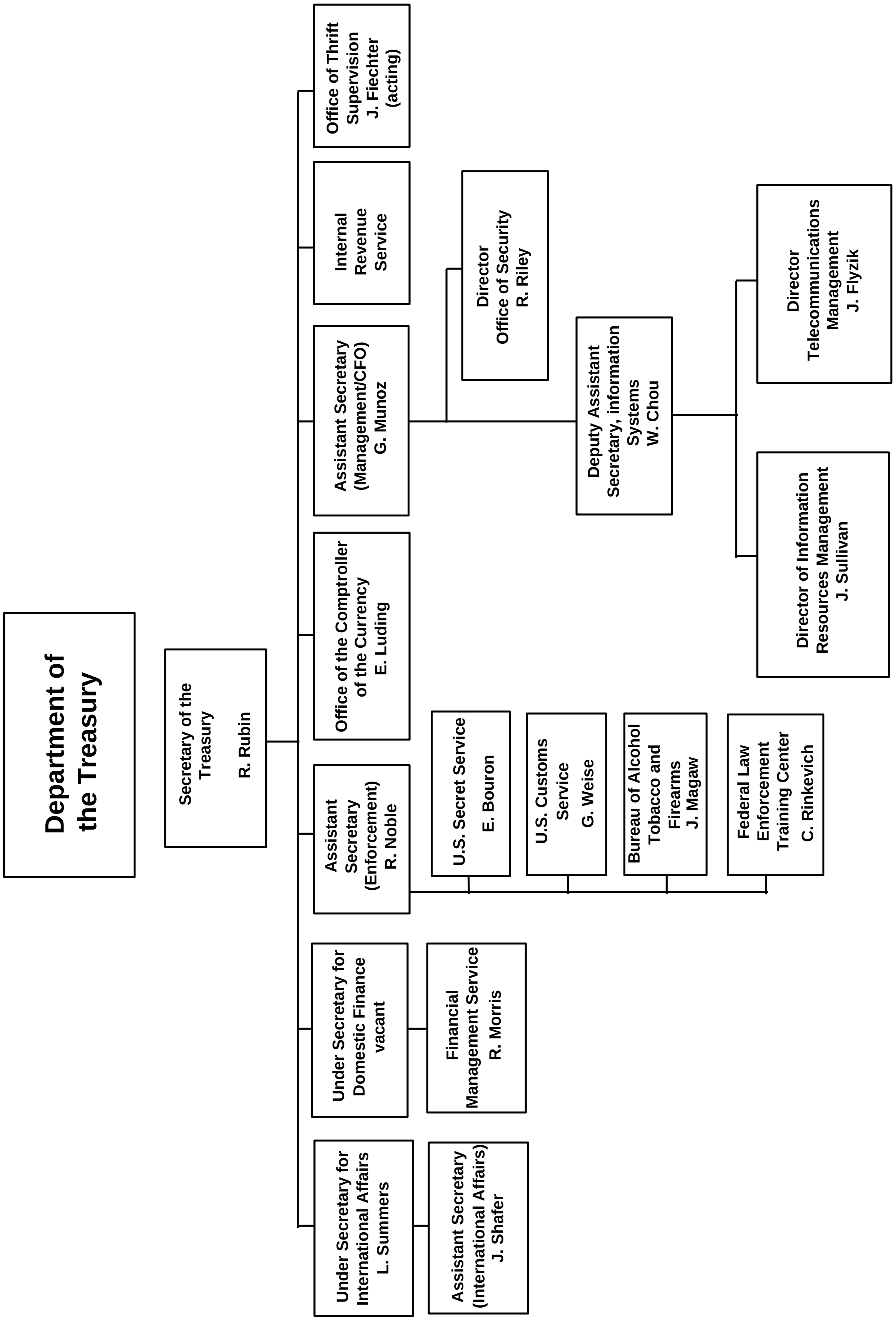
The Director of the Information and Technology Directorate (G-SI) is the USCG Chief Information Officer. Primary responsibility for information security policy lies with the Office of Information Management (G-SII) in G-SI.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- With respect to IW, the biggest issue for the Coast Guard is interoperability. Standard operations for the Coast Guard do not mirror DoD when it comes to standardized equipment, procedures, communications assets, or communications paths. The Coast Guard has limited access to MILSATCOM, but current bandwidth does not fulfill data requirements. Navy and Coast Guard have similar information requirements, especially when operating jointly. Near real-time requirements for unique missions have forced the Coast Guard to seek commercial satellite alternatives.
- The Coast Guard supports national security interests but not in the same sense as DoD. The Coast Guard has no organizational definition of IW, and even if it did, it is likely it would differ from the DoD definition. An example of a national security interest which directly involves the Coast Guard is the migrant issue. Migrants are an issue to the State Department, but is not as identifiable with DoD.

- Another key issue which distinguishes the Coast Guard from DoD is the origination of classified information. The Coast Guard has limited authority to originate classified information. Most classified information handled by the Coast Guard is derivative in nature. However, most information on Coast Guard unique missions (Maritime Law Enforcement, Search and Rescue, etc.) can be handled at the unclassified but sensitive level.
- The Coast Guard is developing a C4I architecture which will encompass all aspects of C4I and sensors.
- The Coast Guard is planning full migration to the Defense Message System (DMS). The transition plan is currently under development.

This page intentionally left blank.


Department of the Treasury
Secretary of the Treasury
R. Rubin
Under Secretary for International Affairs
L. Summers
Assistant Secretary (International Affairs)
J. Shafer
Under Secretary for Domestic Finance
vacant
Financial Management Service
R. Morris
Assistant Secretary (Enforcement)
R. Noble
U.S. Secret Service
E. Bouron
U.S. Customs Service
G. Weise
Bureau of Alcohol Tobacco and Firearms
J. Magaw
Federal Law Enforcement Training Center
C. Rinkevich
Office of the Comptroller of the Currency
E. Luding
Assistant Secretary (Management/CFO)
G. Munoz
Director
Office of Security
R. Riley
Deputy Assistant Secretary, informations Systems
W. Chou
Director of Information Resources Management
J. Sullivan
Director
Telecommunications Management
J. Flyzik
Internal Revenue Service
Office of Thrift Supervision
J. Fiechter
(acting)

Organization: Department of the Treasury (Treas)

Senior Information Assurance Official:

G. Munoz, Assistant Secretary for Management and Chief Financial Officer

Information Assurance Points of Contact:

R. Riley, Director, Office of Security
M. Ferris, Systems Security, Office of Security
W. Chou, Deputy Assistant Secretary for Information Systems
J. Sullivan, Director, Office of Information Resources
J. Flyzik, Director, Office of Telecommunications Management

On-Line Resources:

DoTreas Homepage: http://www.ustreas.gov/treasury/Homepage.html
U.S. Secret Service: http://www.ustreas.gov/treasury/bureaus/usss/usss.html
FinCen: http://www.ustreas.gov/treasury/bureaus/fincen/fincen.html
US Customs Service: http://www.ustreas.gov/treasury/bureaus/customs/customs.html

Information Assurance Related Missions and Functions:

The Department of the Treasury formulates and recommends domestic and international economic, financial, tax, and fiscal policies; serves as financial agent of the U. S. Government; enforces Federal statutes; and manufactures coins and currency.

The Secretary serves as the Chief Financial Officer of the U. S. Government, Chairman *pro tempore* of the Economic Policy Council and as U. S. Governor of the International Monetary Fund and the International Bank for Reconstruction and Development, as well as the Inter-American and African Development Banks.

The Assistant Secretary (Enforcement) supervises the Bureau of Alcohol, Tobacco and Firearms (BATF); Federal Law Enforcement Training Center (FLETC); United States Customs Service (USCS); and the United States Secret Service (USSS) and the Financial Crimes Enforcement Network (FinCEN). The Assistant Secretary (Enforcement) is also responsible for the Office of Financial Enforcement and the Office of Foreign Assets Control.

- Aside from the Presidential protection mission, the USSS is responsible for White House security and the security of foreign missions in the United states. The USSS also enforces statutes related to currency, coins, obligations, and securities of the United States and foreign governments; forgery or fraudulent negotiation of Federal government checks, bonds, and other obligations or securities of the United States; criminal violations of the Federal Deposit Insurance Act; electronic funds frauds, credit and debit card frauds, false identification documents or devices, computer access fraud, and U. S. Department of Agriculture food coupons; and others

.

- The USCS collects the revenue from imports and enforces customs and related laws, such as export and technology transfer statutes.

- The BATF enforces and administers firearms and explosives statutes, as well as the statutes concerning producing, taxing and distributing alcohol and tobacco products.

- FLETC provides training for the Department of Treasury. This training is also available to other Federal, state and local police agencies.

The Financial Crimes Enforcement Network (FinCEN) provides a Government-wide, multi-source intelligence and analytical network to support other agencies in detecting, investigating and prosecuting domestic and international money laundering and other financial crimes. FinCEN provides law enforcement with tactical and strategic intelligence analyses that identify emerging trends and geographical patterns of money laundering and suspected offenders. FinCEN provides specially trained investigators who are experienced in analyzing financial records and data and operates a communications center to answer requests from law enforcement agencies for specific data and information.

The Undersecretary of Domestic Finance supervises the administration of the Government’s fiscal affairs including administrating Treasury financing operations; managing Treasury’s cash balances in tax and loan investment accounts in commercial financial institutions, as well as the operating balances of Federal Reserve Banks; and participating in the Joint Financial Management Improvement Program for improving accounting in the Federal government.

- The Financial Management Service provides financial services, information and advice to the Treasury Department, Federal program agencies and Government policy makers. The Service issues Treasury checks and electronic fund transfer payments to meet the Federal payroll, social security, veteran’s benefits, and income tax refunds.

- The Bureau of Public Debt borrows the money needed to operate the Federal government; accounts for the public debt; and issues Treasury securities to refund maturing debt and raise new money.

The Assistant Secretary (International Affairs) advises the Secretary on international monetary, financial, commercial, energy, and trade policies and programs.

The Internal Revenue Service (IRS) administers internal revenue statutes and educates the public as to their rights and responsibilities under these laws.

The Office of the Comptroller of the Currency regulates national banks. This office examines banks and has the power to close banks that are not in compliance. The office also issues rules and regulations.

The Office of Thrift Supervision charters and regulates Federal- and State-chartered thrift institutions belonging to the Savings Association Insurance Fund.

The Inspector General is responsible for providing comprehensive, independent and objective audit and investigation programs to identify and report program deficiencies and improve the economy, efficiency and effectiveness of operations.

The Treasurer of the United States oversees the U. S. Mint and the Bureau of Engraving and Printing. The primary mission of the Mint is to produce an adequate volume of circulating coinage for the Nation to conduct its trade and commerce. The Bureau of Engraving and Printing designs, prints and finishes a wide range of security products, to include Federal Reserve notes, U. S. postage stamps, Treasury securities, identification cards, and certificates. This bureau also assists other Federal agencies in designing and producing documents that require some level of security or counterfeit-deterrence.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Department of the Treasury has approximately 165,000 employees and operates in a decentralized manner. It relies on OMB and GSA guidance for security of sensitive unclassified information.
- Training alone may not be a cost-effective means of improving security.
- The information assurance discussion seems to focus on the vulnerability of telecommunications, but should also be concerned about value-added networks that serve as additional communications infrastructure and which ride on the telecommunications infrastructure.
- The A-130 policy seems to imply that the policy should be “let the buyer beware,” and although there may be some merit in this approach, policy should also establish minimum standards. The Department of the Treasury participates in several *ad hoc* efforts to develop standards.
- The Department, with input from departmental security experts, writes very broad policy for internal implementation. Minimum standard practices are included in the Department’s security manual.
- As seems to be the case Government-wide, there is not much budget available for security efforts.
- The Department is establishing a very extensive communications and data network, the Treasury Communications System, which will rely on commercial telecommunications.
- The Department does not conduct active penetration testing of the Department’s networks. Some Bureaus, such as the IRS, do conduct tests of their own networks.
- The Department continues to be involved in a substantial amount of computer crime investigations. Bob Friel, Financial Crimes, can provide details.

- The Office of the Comptroller of the Currency regulates national banks, the Federal Deposit Insurance Corporation regulates certain banking operations. FEDline is a computer-to-computer encrypted system used for transfers from government activities to the Federal Reserve System (FRS).
- The Department's Telecommunications and Information Security Working Group coordinates information security issues. Information systems security officers conduct certification and accreditation. Security duties included in job descriptions and categories identify personnel who are qualified or experienced in security of specific systems or classes of systems.
- The Department, IRS and Financial Management Service participate in developing banking standards.
- Wireless architecture and security issues are being addressed by the USSS.
- The USSS is continuing to participate in Joint Computer Crime Unit activities. The unit recognizes that hackers share information and tools in the global village that in the hands of a person with malicious intent could be used to cause grave damage to US interests. The unit hopes to preempt such attacks and shares its information in an interagency forum.
- The USSS commented that over the last year there has been a rise in the percentage of outsider attacks on industry versus insider. The proportion is now approximately 40 percent outsider versus 60 percent insider attacks.
- The Secret Service and the FBI have formed a coordination group with several banking associations to combat financial fraud and computer crimes. The banking associations include the Washington-based American Bankers Association, Independent Bankers of America, America's Community Bankers, and the Credit Union National Association. [Washington Technology, May 23, 1996, page 8]

Interagency Groups

Interagency Groups

This page intentionally left blank.

Federal Agency Computer Security Program Managers' Forum

Co-Chairs

S. Pitcher, DoC

E. Roback, NIST

Organization: Federal Agency Computer Security Program Managers' Forum

Senior Information Assurance Official:

Information Assurance Points of Contact:

Sadie Pitcher, Department of Commerce, Co-Chair
Ed Roback, National Institute of Standards and Technology, Co-Chair

On-Line Resources:

Information Assurance Related Missions and Functions:

The Federal Agency Computer Security Program Managers' Forum sponsored by NIST is an informal government interagency organization for advocacy and information exchange on computer security issues among Federal departments and agencies. The Federal Agency Computer Security Program Managers' Forum addresses issues related to the security of unclassified federal computer and telecommunications systems (except "Warner Amendment" systems as described in 44 U.S.C. Section 3502).

The Managers' Forum has no legal or regulatory basis as such, but rather, was created out of need by NIST. The Managers' Forum is mainly an information-sharing body, though its charter was recently changed to make it into a more proactive group.

Membership includes the following organizations. Where a subordinate organization is indicated, both the parent and subordinate organizations may join as members.

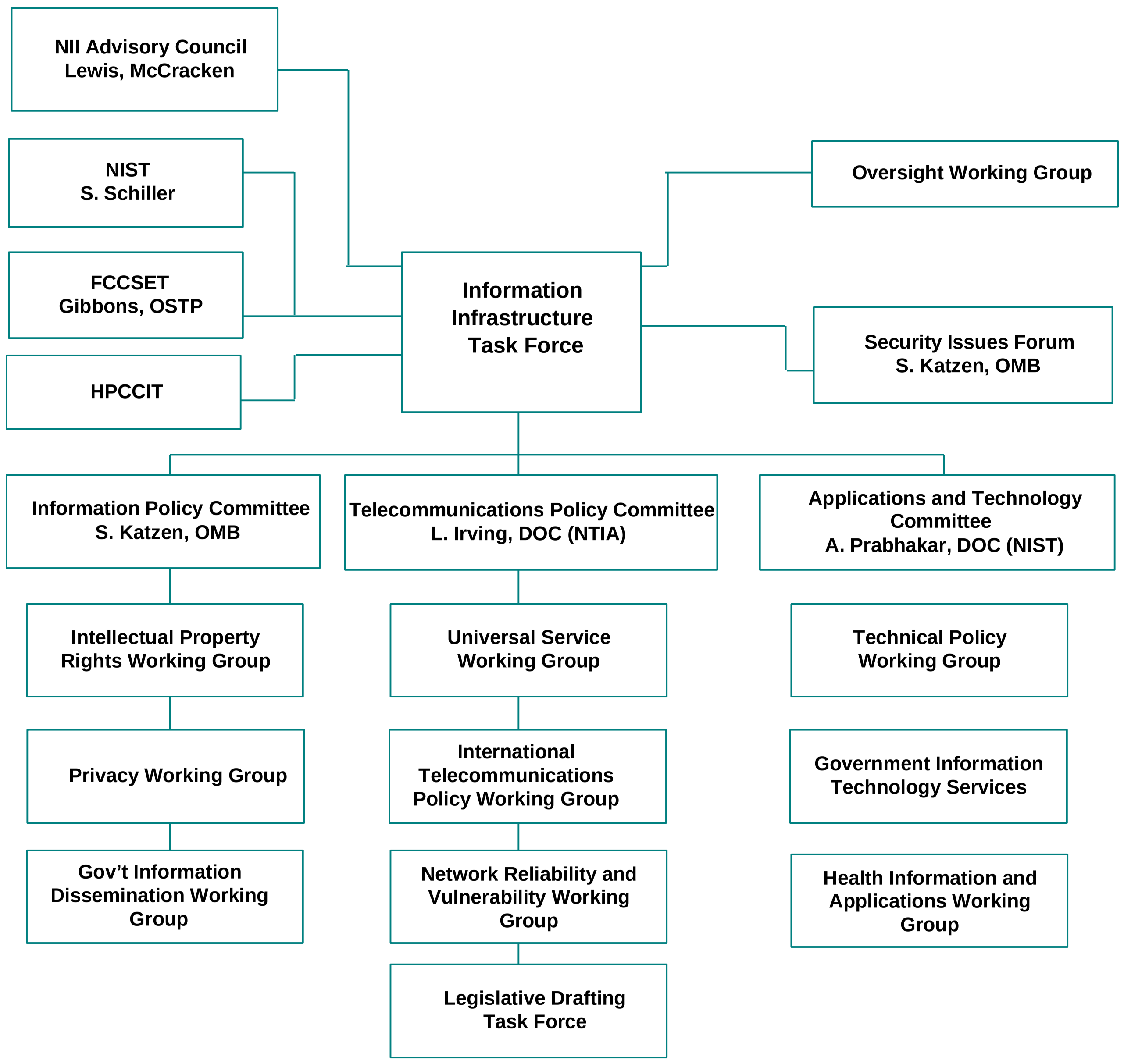
Agency for International Development
Commodity Futures Trading Commission
Department of Agriculture
  Federal Crop Insurance Corporation
Department of Agriculture
  Agricultural Marketing Service
Department of Commerce
  Patent and Trademark Office
Department of Commerce
  National Oceanographic and Atmospheric Administration
Department of Commerce
  Bureau of the Census
Department of Education

- Department of Energy
  - Federal Energy Regulatory Commission
- Department of Health & Human Services
  - Public Health Service
  - Health Care Financing Administration
  - Administration for Children & Families
- Department of Housing & Urban Development
- Department of Interior
  - Bureau of Land Management
- Department of Justice
  - Federal Bureau of Investigation
  - Immigration and Naturalization Service
- Department of Labor
  - Employment & Training Administration
  - Office of the Solicitor
  - Employment Standards Administration
  - Occupational Safety & Health Administration
  - Office of Administrative Law Judges
  - Bureau of Labor Statistics
  - Pension & Welfare Benefits Administration
  - Veterans Employment & Training Service
- Department of State
  - Bureau of Diplomatic Security
- Department of Transportation
  - Federal Railroad Administration
  - Maritime Administration
  - Federal Transit Administration
  - Research & Special Programs Administration
  - Federal Highway Administration
  - U.S. Coast Guard
  - National Highway Traffic Safety Administration
  - Federal Aviation Administration
- Department of Treasury
- Department of Veterans Affairs
  - IRM, Plan., Acq. & Security Service
- Environmental Protection Agency
- Equal Employment Opportunity Commission
- Executive Office of the President
- Farm Credit Administration
- Federal Communications Commission
- Federal Deposit Insurance Corporation
- Federal Emergency Management Agency
- Federal Maritime Commission
- General Accounting Office

General Services Administration
House of Representatives
    House Information Systems
Library of Congress
National Aeronautics & Space Administration
National Institute of Standards and Technology
National Labor Relations Board
National Science Foundation
National Security Agency
Nuclear Regulatory Commission
Office of Management and Budget
Office of Personnel Management
Resolution Trust Corporation
Securities and Exchange Commission
Small Business Administration
Social Security Administration
U.S. Information Agency
U.S. Senate
    Data Security Administrator
U.S. Supreme Court

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Forum is primarily an information sharing group, but has established some working groups on best practices and system access rules.
- The Forum holds an annual off-site meeting to concentrate on current security issues.


NII Advisory Council
Lewis, McCracken
NIST
S. Schiller
FCCSET
Gibbons, OSTP
HPCCIT
Information
Infrastructure
Task Force
Oversight Working Group
Security Issues Forum
S. Katzen, OMB
Information Policy Committee
S. Katzen, OMB
Telecommunications Policy Committee
L. Irving, DOC (NTIA)
Applications and Technology
Committee
A. Prabhakar, DOC (NIST)
Intellectual Property
Rights Working Group
Privacy Working Group
Gov't Information
Dissemination Working
Group
Universal Service
Working Group
International
Telecommunications
Policy Working Group
Network Reliability and
Vulnerability Working
Group
Legislative Drafting
Task Force
Technical Policy
Working Group
Government Information
Technology Services
Health Information and
Applications Working
Group

Organization: Information Infrastructure Task Force

Senior Information Assurance Official:

Secretary of Commerce

Information Assurance Points of Contact:

Information Policy Committee: Bruce McConnell
Intellectual Property Rights WG: Edward Kazenske
Privacy Working Group: Jerry Gates
Government Information WG: Peter Weiss

Telecom. Policy Committee: Tatia Williams
Universal Service Working Gp: Tatia Williams
Rel. and Vul. Working Gp: James Fletcher
Int. Telecom. Working Gp: Sharon Bywater
Legislative Drafting TF: Ellen Bloom

Committee on Appl's and Tech.: Cita Furlani
Gov't Info. Tech. Svcs (GITS): Jim Flyzik
Tech. Policy WG: Howard Frank
Health Info. and Appl's WG: John Silva

NII Security Issues Forum: Glenn Schlarman

Access to IITF Bulletin Board: 202/501-1920
IITF Secretariat: Susannah Schiller
IITF Committee Report: Susannah Schiller

On-Line Resources:

IITF Homepage: http://iitf.doc.gov/

Information Assurance Related Organizations, Missions and Functions:

The Clinton Administration formed the Information Infrastructure Task Force (IITF) to articulate and implement the Administration's vision for the National Information Infrastructure (NII). The task force consists of high-level representatives of the Federal agencies that play a major role in the development and application of information and telecommunications technologies.

Working together with the private sector, the participating agencies will develop comprehensive technology, telecommunications, and information policies and promote applications that best meet the needs of both the agencies and the country. By helping build consensus on difficult policy issues, the IITF will enable agencies to make and implement policy more quickly and effectively.

There are three IITF Committees: Information Policy Committee, Telecommunications Policy Committee, and a Committee on Applications and Technology.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- A number of the IITF's subordinate efforts have, or will soon be, concluded. It is expected that a new smaller structure for the IITF will be proposed. The major areas of emphasis for continuing IITF activities will be health care, privacy, emergency management and public safety, security, and support of GII initiatives.

Organization: Security Issues Forum, IITF

Senior Information Assurance Official:

Salley Katzen, Chairperson, SIF

Information Assurance Points of Contact:

Glenn Schlarman

Information Assurance Related Missions and Functions:

The NII Security Issues Forum will provide leadership for Federal NII security activities. It will ascertain the security needs of the various NII user communities and the Federal role in assuring such security. It will ensure coordination of the security activities across the various Committees of the IITF and serve as a clearinghouse for Federal security efforts related to the NII. The Forum will also consider the scope of legal and policy remedies necessary to achieve desired security in the NII.

The Forum coordinates the following IITF activities:

- Telecommunications Policy Committee (TPC), the Information Policy Committee (IPC), and the Committee on Applications and Technology (CAT).
- Intellectual Property Rights Working Group (IPRWG) and the Privacy Working Group (PWG).
- The Government Information Technology Services Working Group (GITS), will advise the Forum on security issues pertaining to the application of information technology by Federal agencies to improve service delivery and accomplish agency missions.

The Forum also coordinates the efforts of the following Federal government entities:

- National Institute of Standards and Technology (NIST) will encourage the Computer System Security and Privacy Advisory Board (CSSPAB).
  NIST, will assess where research and development on security technology would be useful for the NII.
- NIST, working with other agencies, will identify Federal security products, techniques, and practices that will be useful in the NII.
- NIST will work with the Forum of Incident Response and Security Teams (FIRST) to assess how private entities conduct emergency response and how the efforts of Government can be coordinated with them to ensure a "911" capability for the NII.
- National Communications System (NCS), in coordination with the industry's National Security Telecommunications Advisory Committee (NSTAC), will work with the Reliability and Vulnerability Working Group to ensure that National

Security and Emergency Preparedness (NS/EP) needs are accommodated in the NII.

- National Security Telecommunications and Information Systems Security Committee (NSTISSC) will identify useful security tools and techniques in the national security community that may be applicable to the NII.
- Working Group on Encryption and Telecommunications (WGET) will develop policy recommendations regarding the Government's response to the spread of digital telecommunications equipment and inexpensive encryption devices which could prevent effective wiretaps.
- The High Performance Computing and Communications (HPCC) Program will assure development and testing of new technologies for computer security suitable to a high performance environment.
- The Federal Network Council (FNC), a multi-agency committee that oversees Federal research networks, shall explore specific issues relating to security of the Internet.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- SIF has published a draft report, “NII Security: The Federal Role.” The plan will be based on the series of public meetings on NII security held by the SIF. The plan will be subjected to public discussion. It will address security concerns, how to meet the concerns (market forces, private investment, government investment, etc.), legislative proposals, and a possible need for a Federal government response and recovery plan.
- At a March 1996 meeting, the forum decided to focus it efforts on the following three issues:
  - Cryptography policy
  - Infrastructure Assurance
  - Assess the need for assurance for security products and who should do it.
- Regulatory oversight provides an opportunity to influence security in the infrastructures. While government regulatory activity is being reduced, regulation of information technology and security practices might have to increase.

Organization: Reliability and Vulnerability Working Group, IITF

Senior Information Assurance Official:

Information Assurance Points of Contact:

James Fletcher

Information Assurance Related Missions and Functions:

The RVWG has established four subgroups:

Reliability for General Users: This group is addressing issues related to overall NII reliability for Government, industry, and general users in the context of both day-to-day and emergency operations. It has identified strategies for ensuring reliability.

National Security and Emergency Preparedness: This group is addressing issues related to the NS/EP attributes the NII should support. This effort includes reviewing key industry segments such as the public switched network, cable, wireless, satellite, and broadcast and identifying features and capabilities that should be available over the NII to support NS/EP users.

Protection of the Network: This group is addressing issues related to protecting key network elements from unauthorized intrusion or manipulation and is seeking to ensure that network management information is protected. It is developing a report that will describe the potential challenges to protecting the network in the evolving NII, the threats to and vulnerabilities of the network, the resulting risks to the NII, and current efforts to reduce risks. It will conclude with an approach for addressing the system protection problem in the NII.

Integration and Planning: This group has taken inputs from each of the other subgroups and melded them into a proposed action plan that addresses reliability and vulnerability concerns. The plan describes problems, as well as key issues and necessary actions, in the areas of policy, legislation, management mechanisms, and technology. The subgroup will accomplish its objective by using an integrating framework that is currently in draft and is being addressed by the RVWG.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The RVWG has issued a report entitled *"NII Risk Assessment: A Nation's Information at Risk."* The report concluded that:
  - There are real and active threats to the NII and those threats will grow over time.
  - There is not enough information available to conduct a more rigorous analysis of the NII.
  - There is no common framework, approach, or terminology for discussing or analyzing risks to the NII.
  - No sound mechanism exists for government and industry to share information necessary for future sound risk assessments on individual systems.
  - Risk management must be a coordinated effort involving many different activities.
  - Because the NII is so broad and complex, its risk can only be assessed at a high level.
- The emphasis of the reports recommendations were centered on the need to establish mechanisms to support information exchange between all NII users detailing how they use the NII, how the risks to the NII will affect them, and what to do to manage those risks.
- The RVWG has formally declared the conclusion of its activities and is expected to disband within the next year.
- The RVWG has also established a working relationship with the President's National Security Telecommunications Advisory committee (NSTAC) through its NII Task Force. The RVWG subgroup leaders met with the Chairs of the NII Task Force and its three subgroup chairs to discuss issues of mutual interest and to determine how to make their efforts complementary. RVWG representatives, including the subgroup leaders, have attended meetings of the NII Task Force to continue the dialogue between the two organizations. In particular, the RVWG NS/EP subgroup has met with the NSTAC NII Task Force Architecture Subgroup and factored industry's input into its efforts to identify NII NS/EP features and capabilities.
- The RVWG determined that its overall objective was to ensure that telecommunications services and information systems of the national information infrastructure will provide: high quality service for normal operations; maximum reliability of services to meet essential public, private, and commercial needs; and capabilities that meet national security and emergency preparedness requirements. The working group agreed that the best approach to achieve that objective would be to focus on top level actions that address its span of responsibilities. The proposed Plan of Action identifies top level actions that will be pursued by the RVWG, in partnership with industry and government user groups. The plan recommends tasking for specific government agencies, recommends tasking to and from other IITF committees and working groups, and develops strategies to leverage industry and other user groups to accomplish these actions.
- The Group is developing a Reliability and Vulnerability Working Group Work Plan. The RVWG subgroups have been reviewing the proposed actions and identifying milestones to accomplish those actions. For each milestone, they are setting target dates and proposing candidate offices of primary responsibility. The RVWG plans to reach consensus on its Plan of Action. It is expected that the Plan of Action will be a "living document," capable of responding to the dynamic NII environment.

Organization: Information Management Policy Working Group

Senior Information Warfare Official:

Information Warfare Points of Contact:

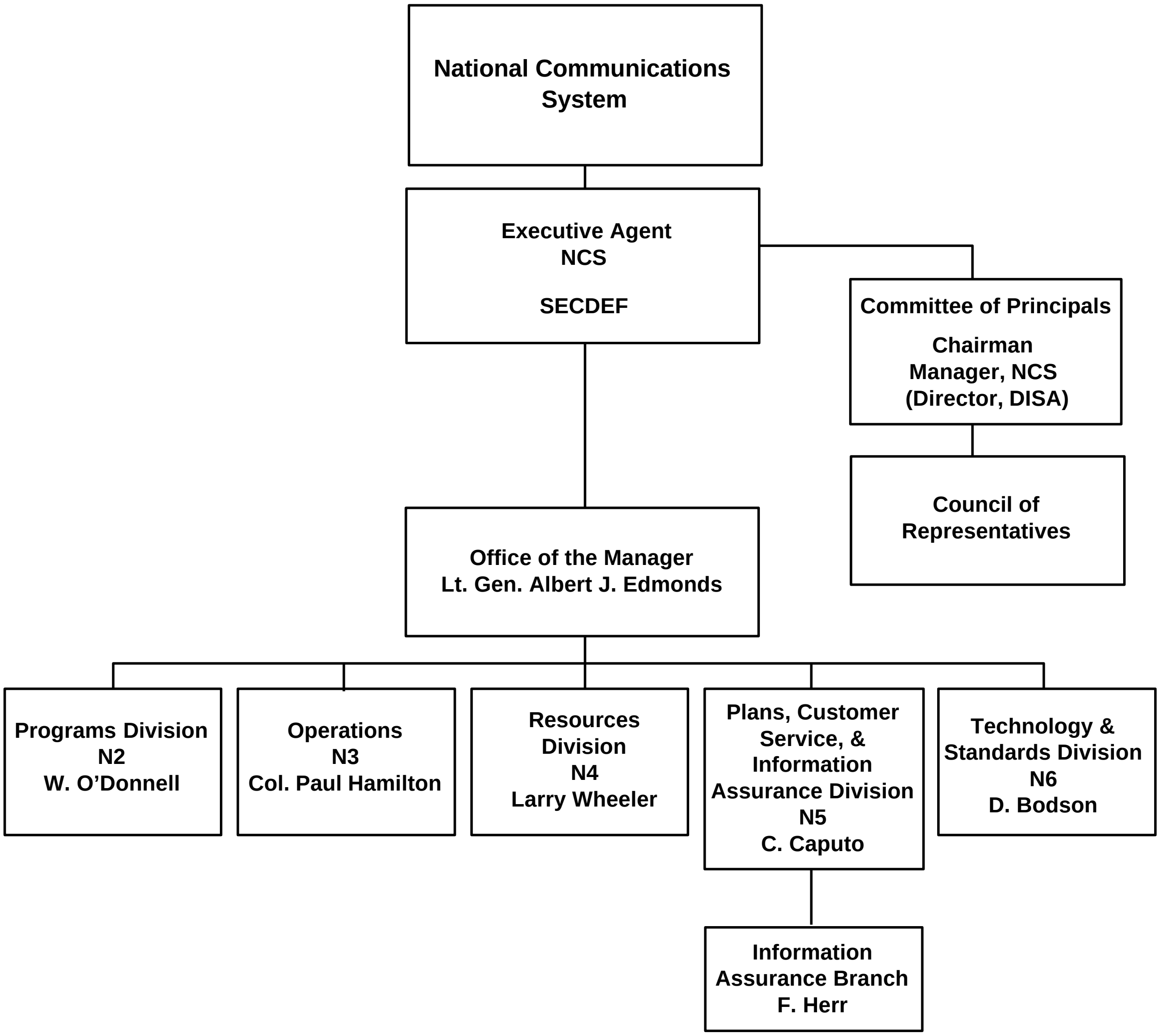
On-Line Resources:

Information Warfare Related Missions and Functions:

The IMPWG is a joint DoD/DCI group created to support the Information Systems Board (ISB). Chaired by the Executive Director for Intelligence Community Affairs and the Deputy Assistant Security of Defense (Intelligence and Security), the ISB advises the DCI and the Deputy Secretary of Defense on information security matters as they pertain to interaction among organizations under their purview. The IMPWG, in turn, establishes automated intelligence information systems management and associated security policy and programs. The mission of IMPWG is to recommend top-level architectures; adopt community standards; develop policy to effect connectivity and common-user infrastructure, and interoperability; provide program and budget support; and provide liaison and coordination on security and technology issues.

Membership consists of DIA, CIA, NSA, CIO, Joint Staff, NRO, Military Services, DMA, DISA, State, Treasury, DoE, FBI, Commerce, and additional organizations as necessary. Accomplishments of the IMPWG include devising and issuing a security risk assessment methodology.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:


National Communications System
Executive Agent NCS SECDEF
Committee of Principals Chairman Manager, NCS (Director, DISA)
Council of Representatives
Office of the Manager Lt. Gen. Albert J. Edmonds
Programs Division N2 W. O'Donnell
Operations N3 Col. Paul Hamilton
Resources Division N4 Larry Wheeler
Plans, Customer Service, & Information Assurance Division N5 C. Caputo
Technology & Standards Division N6 D. Bodson
Information Assurance Branch F. Herr

Organization: National Communications System (NCS)

Senior Information Assurance Official:

Lieutenant General Al Edmonds, Manager, NCS

Information Assurance Points of Contact:

Fred Herr, Office of the Manager, NCS

On-Line Resources:

NCS Homepage: http://164.117.147.223/

Information Assurance Related Missions and Functions:

The Interdepartmental Committee on Communications was formed by the National Security Council on October 26, 1962, to resolve the major communications problems which had surfaced during the Cuban missile crisis. The Committee's work resulted in the creation of the NCS on August 21, 1963. The NCS was updated by Executive Order 12472, April 3, 1984, and is charged with assisting the President, the National Security Council, the Office of Science and Technology Policy, and the Office of Management and Budget in the exercise of their wartime and non-wartime emergency telecommunications functions, and their planning and oversight responsibilities. The NCS also assists in the coordination of planning for and the provision of national security and emergency preparedness telecommunications of the Federal government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. In addition, the Office of the Manager, NCS (OMNCS), provides administrative support to the President's National Security Telecommunications Advisory Committee.

Membership includes:

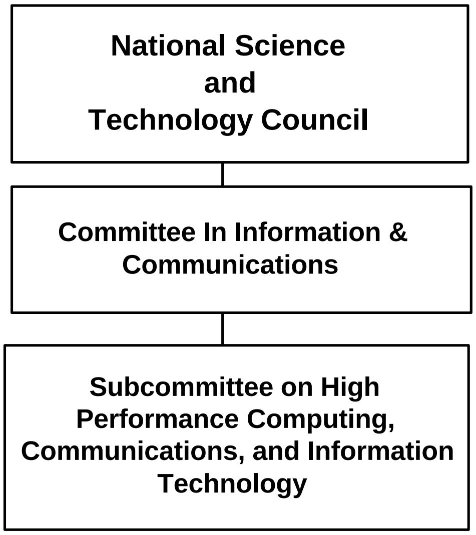
Department of Agriculture
Department of Commerce
Department of Defense
Department of Energy
Department of Health and Human Services
Department of Justice
Department of State
Department of the Interior
Department of the Treasury
Department of Transportation
Department of Veterans Affairs
Central Intelligence Agency
Federal Communications Commission

Federal Emergency Management Agency
Federal Reserve System
General Services Administration
The Joint Staff
National Aeronautics and Space Administration
National Security Agency
National Telecommunications and Information Administration
Nuclear Regulatory Commission
United States Information Agency
United States Postal Service

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- GETS. The Government Emergency Telecommunications Service provides National Security/Emergency Preparedness (NS/EP) users with dependable and flexible switched voice and voice-band data communications during times of extreme emergency or war. GETS derives its service from the assets and capabilities of the Public Switched Network (PSN). This emergency telecommunications service is provided by a variety of techniques. One technique is to restrict access to the priority services to only NS/EP users. Another technique is to provide priority treatment for GETS calls in the form of priority trunk queuing and reservation, exemption from restrictive management controls (e.g., call blocking) imposed during periods of excessive network loading, and the use of a special NS/EP identifier for priority call identification and call set up. Finally, routing of the NS/EP calls through the network is accomplished by an enhanced process which increases the number of possible routes searched -- in normal operations, a trunk busy signal is returned to the originator of the call in the event the signaling system makes three unsuccessful attempts to find a route to the call destination.
- The current GETS requirements and operational concept are based on six functional requirements for NS/EP telecommunications that were defined in an Executive Office of the President Memorandum (dated October 15, 1991) on the National Level Telecommunications Program Implementation and Functional Requirements.
- The Government Emergency Telecommunications Service (GETS) achieved its initial operating capability on 1 October 1995.
- High Probability of Completion (HPC) is an American National Standards Institute (ANSI) SS7 network capability standard (ANSI T1.631-1993) for identification of NS/EP calls in SS7 networks creating a means for identifying GETS traffic within the Public Switched Network (PSN) on a call-by-call basis and triggering the activation of priority treatment and other enhancements.
- The NCS managed Telecommunications Service Priority System (TSP) establishes the regulatory, administrative, and operational framework to authorize the priority provisioning and restoration of NS/EP telecommunications services. This allows vendors to initiate, restore, or otherwise act on a priority basis to ensure effective NS/EP telecommunications.

- The Director, NSA, briefed the National Security Telecommunications Advisory Committee (NSTAC) in January 1995 on the threat really pushing NSTAC/NCS model for other industries. Director FBI also spoke to NSTAC after recent Executive Session. IES members met with CAPT Dave Henry and Mr. Dave Patterson of NSA to discuss threat. Jack Edwards briefed NSTAC response to McConnell briefing at last NSTAC meeting.
- Have briefed J33 and J6 on on-going efforts. Also briefed personnel from the Office of the Secretary of Defense (OSD) Net Assessment and Office of the Under Secretary of Defense Policy (USD(P)).
- National Defense Infrastructures Survivability Study by USD(P) is underway. Being done by DNA as a successor to the Key Asset Protection Program (KAPP).
- NII Symposium conducted at NWC in Newport last October.
- Bellcore has 5-year contract with OMNCS to collect Public Switched Network (PSN) vulnerability and incident data. The data collected will build on Bellcore's Security Information Exchange data.
- SRI has produced hacker profile for OMNCS.
- The February 1996 NSTAC focused on IA with briefings by Deputy Attorney General, Jamie Goulick; Secretary Policy Board Staff Director, Peter Soderholm; Center for Strategic & International Studies; Director, Arnaud De Borchgrave; and Jeffrey Symoth, General Counsel, CIA. Senator Jon Kyl, author of the Kyl Amendment to the Defense Authorization Bill spoke to NSTAC during the Executive Breakfast.


National Science and Technology Council
Committee In Information & Communications
Subcommittee on High Performance Computing, Communications, and Information Technology

Organization: National Science and Technology Council

Senior Information Assurance Official:

Information Assurance Points of Contact:

On-Line Resources:

NSTC Homepage:
http://www.whitehouse.gov/WH/EOP/OSTP/NSTC/html/NSTC_Home.html

Information Assurance Related Missions and Functions:

President Clinton established the National Science and Technology Council (NSTC) by Executive Order 12881 on November 23, 1993. This cabinet-level council is the principal means for the President to coordinate science, space, and technology policies across the Federal government.

An important objective of the NSTC is the establishment of clear national goals for Federal science and technology investments in areas ranging from information technologies and health research, to improving transportation systems and strengthening fundamental research. The Council prepares research and development strategies that are coordinated across Federal agencies to form an investment package that is aimed at accomplishing multiple national goals.

<u>Membership</u>:
The President
The Vice President
Secretary of State
Secretary of Defense
Secretary of Interior
Secretary of Agriculture
Secretary of Commerce
Secretary of Labor
Secretary of Health and Human Services
Secretary of Transportation
Secretary of Energy
Secretary of Education
Director, Office of Management and Budget
Assistant to the President for Science and Technology
Assistant to the President for National Security Affairs
Assistant to the President for Economic Policy

Assistant to the President for Domestic Policy
Chair of the Council of Economic Advisors
Administrator, National Aeronautics and Space Administration
Administrator, Environmental Protection Agency
Director, National Science Foundation
Director, National Institutes of Health
Director, Central Intelligence Agency
Director, Arms Control and Disarmament Agency

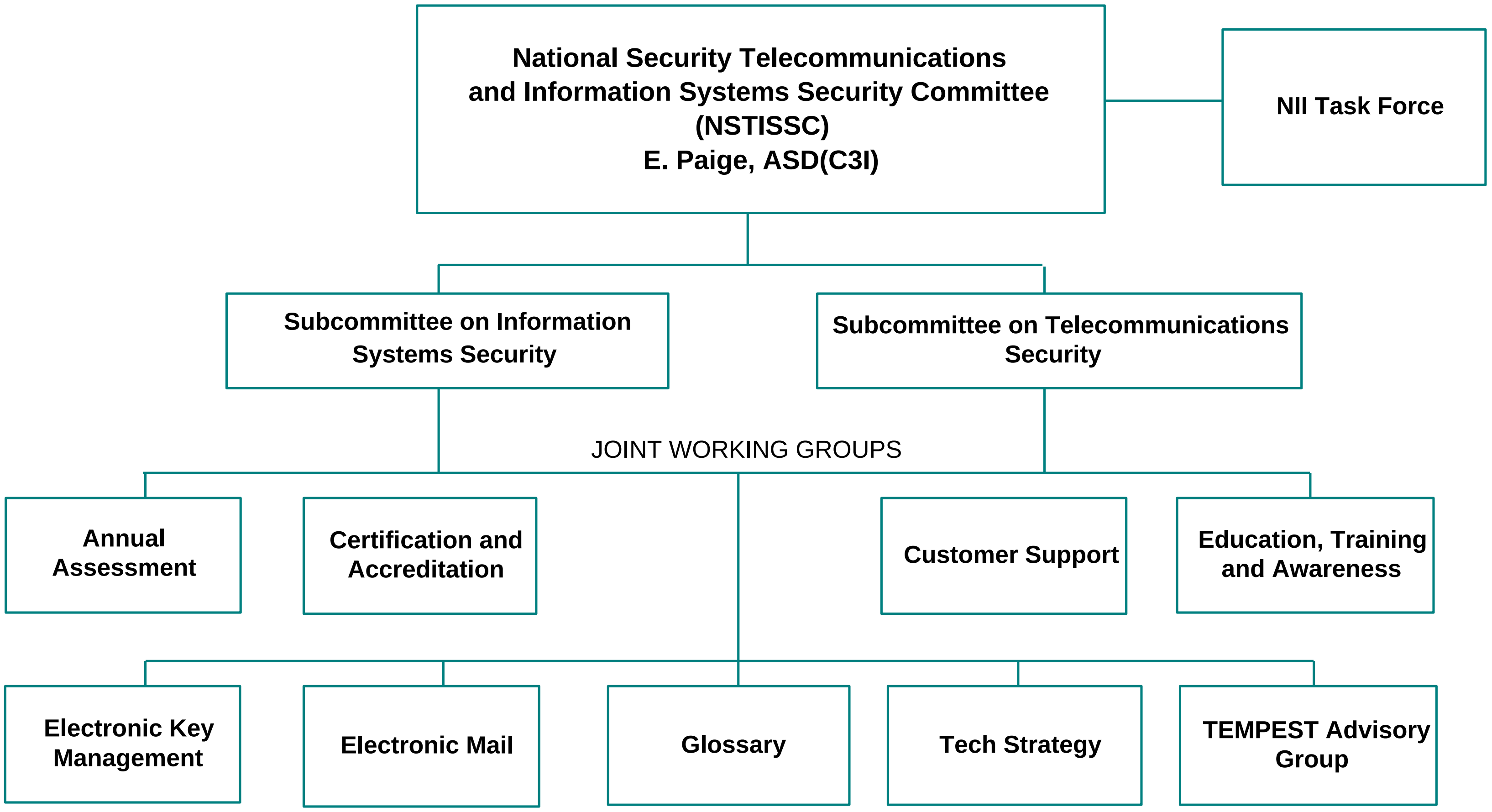
President Clinton directed the NSTC to:

- Coordinate the science and technology policy making and implementation process across Federal agencies;
- Ensure that science and technology policy decisions are consistent with the President's stated goals;
- Ensure that science and technology issues are considered in the development and implementation of Federal policies and programs;
- Further international cooperation in science and technology activities.

The Council fosters a strategic approach in determining how science and technology can help resolve complex societal needs. Today's problems demand contributions from different fields of study and a team approach from the agencies that make up the Federal R&D enterprise. The NSTC provides an interagency strategic management system to foster teamwork and enhance the ability to identify opportunities for interdisciplinary solutions.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

This page intentionally left blank.



National Security Telecommunications and Information Systems Security Committee (NSTISSC)
E. Paige, ASD(C3I)

NII Task Force

Subcommittee on Information Systems Security

Subcommittee on Telecommunications Security

JOINT WORKING GROUPS

Annual Assessment

Certification and Accreditation

Customer Support

Education, Training and Awareness

Electronic Key Management

Electronic Mail

Glossary

Tech Strategy

TEMPEST Advisory Group

Organization: National Security Telecommunications and Information Systems Security Committee (NSTISSC)

Senior Information Assurance Official:

E. Paige, Assistant Secretary of Defense (C3I), Chairman

Information Assurance Points of Contact:

NSTISSC Secretariat (Located at NSA)

On-Line Resources:

Information Assurance Related Missions and Functions:

NSTISSC was created via NSD 42, dated 5 July 1990. NSD 42 established a senior level policy coordinating committee under the NSC, an interagency group at the operating level (NSTISSC), two subcommittees (one for information systems security and one for telecommunications security), an executive agent (DoD), and a national manager (NSA). The Policy Coordinating Committee provide a “tie breaking” decision when issues cannot be resolved at the NSTISSC level. The Policy Coordinating Committee has been required to meet on only one occasion in the NSTISSC’s history. The NSTISSC’s mission is to consider technical matters and develop operating policies, guidelines, instructions, and directives, as necessary to implement the provisions of the Directive. Specific matters are addressed by joint working groups as required.

The NSTISSC’s National Information Infrastructure (NII) Executive Committee and the NII Task Force (NIITF) were established to develop and implement a comprehensive and proactive program in support of the NII. The Executive Committee provides guidance and direction to the NIITF, oversees its activities, maintains liaison with NIST, as appropriate, and reports periodically to the NSTISSC on its progress. The NIITF is comprised of individuals representing NSTISSC member and observer organizations and is responsible for all NSTISSC support to the NII including:

- Facilitating liaison with various NII fora
- Coordinating the activities of NSTISSC Sub working groups in support of the NII
- Developing white papers on security issues of concern to the NII
- Providing an analysis of the common security services and requirements of member organizations
- Publishing an annual compendium of government information safeguard requirements
- Developing and implementing a campaign to increase awareness of security issues.

NSTISSC membership is categorized as follows:

- Member on the NSTISSC, STS, and SISS
- Observer on the NSTISSC, STS, and SISS
- Observer on the STS and SISS
- Observer on the STS
- Observer on the SISS
- Working Group Member

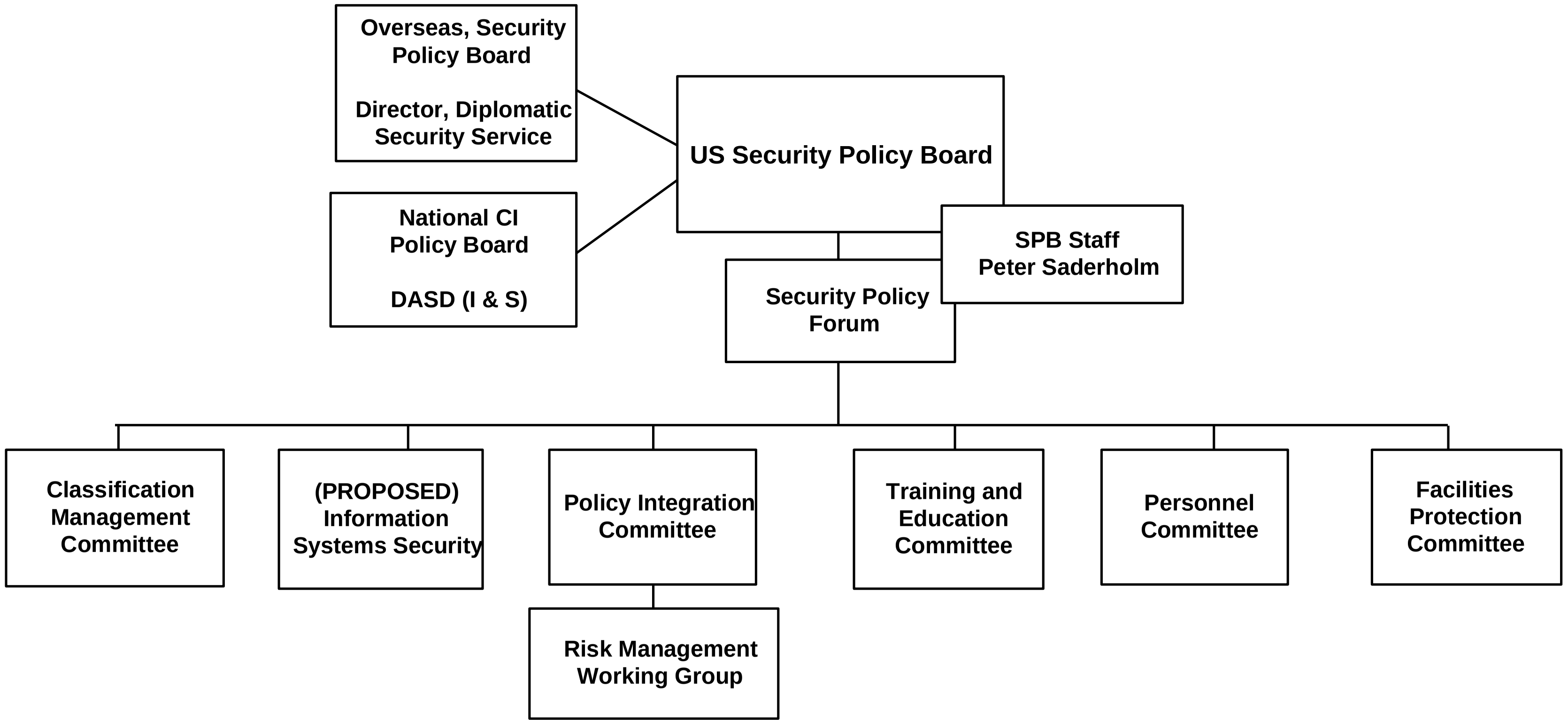
Membership in the various categories includes the following organizations. Details of which members belong to which categories can be obtained from the NSTISSC Secretariat. Where both a parent and subordinate organization are shown, both organizations participate in one or more of the above categories.

National Security Council Staff
Office of Management and Budget
U.S. Department of Agriculture
Department of Commerce
National Institute of Standards and Technology
Department of Defense
Joint Staff
Army
Navy
Marine Corps
Air Force
Defense Information Systems Agency
White House Communications Agency
Defense Intelligence Agency
Defense Investigative Service
Defense Logistics Agency
Defense Mapping Agency
Defense Nuclear Agency
National Security Agency
Department of Education
Department of Energy
Department of Health and Human Services
Indian Health Service
Public Health Service
Department of Housing and Urban Development
Department of the Interior
Department of Justice
Drug Enforcement Administration
Federal Bureau of Investigation
Immigration and Naturalization Service
Department of Labor

Department of State
Department of Transportation
Federal Aviation Administration
U.S. Coast Guard
Department of the Treasury
U.S. Customs Service
U.S. Secret Service
Department of Veterans Affairs
Director of Central Intelligence/Central Intelligence Agency
Federal Communications Commission
Federal Emergency Management Agency
Federal Reserve System
General Services Administration
National Aeronautics and Space Administration
National Communications System
Nuclear Regulatory Commission
Office of Personnel Management
Securities Exchange Commission
U.S. Information Agency

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- NSTISSC accomplishments to date include the development of policies, guidelines, instructions, and standards; provided systems security guidance; produced the annual assessment of the “health” of national security systems; provides release approvals to foreign governments and international organizations; maintained the national issuance system; and produced special publications.


Overseas, Security Policy Board
Director, Diplomatic Security Service
National CI Policy Board
DASD (I & S)
US Security Policy Board
SPB Staff Peter Saderholm
Security Policy Forum
Classification Management Committee
(PROPOSED) Information Systems Security
Policy Integration Committee
Risk Management Working Group
Training and Education Committee
Personnel Committee
Facilities Protection Committee

Organization: United States Security Policy Board (USSPB)

Senior Information Assurance Official:

Peter Saderholm, Director, USSPB Staff

Information Assurance Points of Contact:

Vicki LaBarre, USSPB Staff
Dan Knauf, USSPB Staff

On-Line Resources:

Information Assurance Related Missions and Functions:

The Secretary of Defense (SECDEF) and the Director of Central Intelligence (DCI) created the Joint Security Commission (Commission) in May 1993 to review the security practices and procedures under their authorities.

The Commission concluded that the problems of fragmentation and inconsistency in security policy development, implementation, and oversight must be resolved in order to make meaningful improvements in the overall effectiveness of US Government security. The commission proposed the creation of a unifying structure to "provide leadership, focus, and direction to the government security communities."

Under PDD-29, the U.S. Security Policy Board became the umbrella under which all the elements of security are organized. It is responsible for not only what to protect (classification management) but also how to protect it (security countermeasures). The Board receives overall policy guidance from the NSC and accepts responsibility for the flow of policy direction both to and from the NSC. Consistent with PDD-29, the Board is assisted by the Security Policy Advisory Board (Advisory Board), the Security Policy Forum (Forum), and various intergovernmental committees and working groups.

Committees and ad hoc working groups organized along security discipline lines support the Forum. The principle committees proposed to support the Board structure include:

- A Personal Security Committee (PSC) to address all personnel security policies, procedures, and practices applicable to US Government departments and agencies;

- A Facilities Protection Committee (FPC) to address all policies, practices and procedures applicable to the protection of US Government and industrial facilities; physical, technical, and TEMPEST;

- A Classification Management Committee (CMC) charged with the development of classification management policy within the context of the overall security policy framework;

- A Training and Professional Development Committee (TPDC) to standardize and coordinate security training, education, and awareness and to achieve efficiencies in the development and delivery of such training, and;

- A Policy Integration Committee (PIC) charged to ensure overarching themes are integrated into all U.S. Government security policy and encourage synergy in the activities of the other standing committees.

- An Information Systems Security Committee - TBD

As of 1 June 1995, all committees have been established except the Information Systems Security Committee. (See attachment.)

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The end of the Cold War has dramatically changed the threats that defined the security policies and procedures for protecting our government's information, facilities and people. While some threats have been reduced, others have remained relatively stable or have increased. Our understanding of the range of issues that affect our national security continues to evolve. Economic issues are of increasing concern and are competing with traditional political and military issues for resources and attention. Technologies, such as those used to create weapons of mass destruction are evolving and proliferating. With this greater diversity of threats, there is wide recognition that the security policies, practices, and procedures developed during the Cold War must be reexamined and changed. We require a new security process based on sound threat analysis and risk management practices. A process which can adapt our security policies, practices and procedures as the economic, political and military challenges to our national interests continue to evolve.
- The Director of Central Intelligence and Secretary of Defense's Joint Security Commission identified four principles which should guide the formulation, evaluation and oversight of our security policy:
    - Our security policies and services must realistically match the threats we face and must be sufficiently flexible to facilitate change as the threats evolve.
    - Our security policies and practices must be consistent and enable us to allocate scarce resources effectively.
    - Our security standards and procedures must result in the fair and equitable treatment of all Americans upon whom we rely to guard our nation's security.
    - Our security policies, practices and procedures must provide the security we need at a price we can afford.
- The National Security Act of 1947, as amended, specifies that is the duty of the National Security Council (NSC) to consider policies on matters of common interest to the departments and agencies of the Government concerned with the national security and to

make recommendations to the president in connection therewith. Consistent with the National Security Act of 1947, the President directed the establishment of a new security policy structure, under the direction of the NSC, for the coordination, formulation, evaluation and oversight of security policy guided by the above principles.

- Nothing in this directive amends or changes the authorities and responsibilities of the members of the Policy Board, including, Director of Central Intelligence (DCI), Secretary of Defense, Secretary of State, Secretary of Energy, Secretary of Commerce, Attorney General, Director of the FBI, Chairman of the Nuclear Regulatory Commission, or Director of the Information Security Oversight Office as contained in the National Security Act of 1947, other existing laws or Executive Orders.
- The President directed the following:
  - The Joint Security Executive Committee established by the Deputy Secretary of Defense and the Director of Central Intelligence was designated the Security Policy Board and directed to report to the President through the Assistant to the President for National Security Affairs. The existing national security countermeasures policy and coordination structure, the National Advisory Group for Security Countermeasures, was thereby abolished and its functions transferred to the Security Policy Board.
  - The Security Policy Board consists of the Director of Central Intelligence, the Deputy Secretary of Defense, Vice Chairman of the Joint Chiefs of Staff, the Deputy Secretary of State, the Under Secretary of Energy, the Deputy Secretary of Commerce, the Deputy Attorney General, one Deputy Secretary from another non-defense related agency and one representative from the Office of Management and Budget and the NSC staff. The additional non-defense agency representative will be rotated on an annual basis and selected by the non-defense agency members of the Security Policy Forum established below. Senior representatives of other Departments and Agencies will be invited members at such times as the Security Policy Board considers security issues germane to their responsibilities.
  - The Chairman of the Security Policy Board was designated by the Assistant to the President for National Security Affairs on behalf of the President.
  - The Security Policy Board considers, coordinates and recommends for implementation to the President, through the Assistant to the President for National Security Affairs, policy directives for U.S. security policies, procedures and practices. The Security Policy Board is the principal mechanism for reviewing and proposing to the NSC legislative initiatives and executive orders pertaining to U.S. security policy, procedures and practices that do not fall under the statutory jurisdiction of the Secretary of State. This Board coordinates the development of interagency agreements and resolve conflicts that may arise over the terms and implementation of these agreements. In coordinating security policy, procedures and practices, the Policy Board ensures that all U.S. Departments and Agencies affected by such decisions are allowed to comment on such proposals.
  - Policy disputes that cannot be resolved by this Board are forwarded to the Principals Committee of the National Security Council.
  - A Security Policy Advisory board was established to serve as an independent and non-governmental advisory body on U.S. security policy. Five members, including

a Chairman, will be appointed by the President for terms of up to three years. As of June 1966, the Chairman and two members have been appointed and are being briefed in preparation for their first meeting. The Chairman will report annually to the President through the Assistant to the President for National Security Affairs on implementation of the four policy principles identified above. The Security Policy Advisory Board will also provide a non-governmental and public interest perspective on security policy initiatives to the Security Policy Board and the intelligence community.

- The Security Policy Forum established under the Joint Security Executive Committee was retained under the Security Policy board to consider security policy issues raised by its members or any other means; develop security policy initiatives and obtain Department and Agency comments on these initiatives for the Policy Board; evaluate the effectiveness of security policies; monitor and guide the implementation of security policy to ensure coherence and consistency; and oversee the application of security policies to ensure that they are equitable and consistent with national goals. Policy Forum membership includes one senior representative from the Office of Secretary of Defense, Joint Chiefs of Staff, each Military Department, including the U.S. Coast Guard, Defense Intelligence Agency, National Security Agency, Central Intelligence Agency, Commerce, Energy, Justice, State, Treasury, Transportation, Federal Bureau of Investigation, National Reconnaissance Office, Federal Emergency Management Agency, General Services Administration, Defense Information Systems Agency/National Communications System, Office of personnel Management, Information Security Oversight Office, Nuclear Regulatory Commission, NASA, Office of Management and Budget, Department of Interior, National Archives, Department of Agriculture, and other agencies representatives as invited by the Security Policy Board Chairman.
- The Security Policy Board and Forum has established interagency working groups as necessary to carry out their functions and ensure interagency input and coordination of security policy, procedures and practices. When the work of the group is concluded, the group is dissolved.
- The existing Department of State Overseas Security Policy Group is hereby designated as, and its functions transferred to, the Overseas Security Policy Board and directed to report to the president through the Assistant to the President for National Security Affairs. The Overseas Security Policy Board is chaired by the Director of the Diplomatic Security Service and its membership consists of representatives from the Department of State, Agency for International Development, CIA, Defense Intelligence Agency, FBI, Commerce, Justice, Treasury, Transportation, National Security Agency, United States Information Agency, Peace Corps, Federal Aviation Administration, Foreign Agricultural Service and the DCI's Center for Security Evaluation, Office of Management and Budget, NASA, Arms Control and Disarmament Agency.
- The Overseas Security Policy Board considers, develops, coordinates and promotes policies, standards and agreements on overseas security operations,

programs and projects which affect all U.S. Government agencies under the authority of a chief of mission abroad.

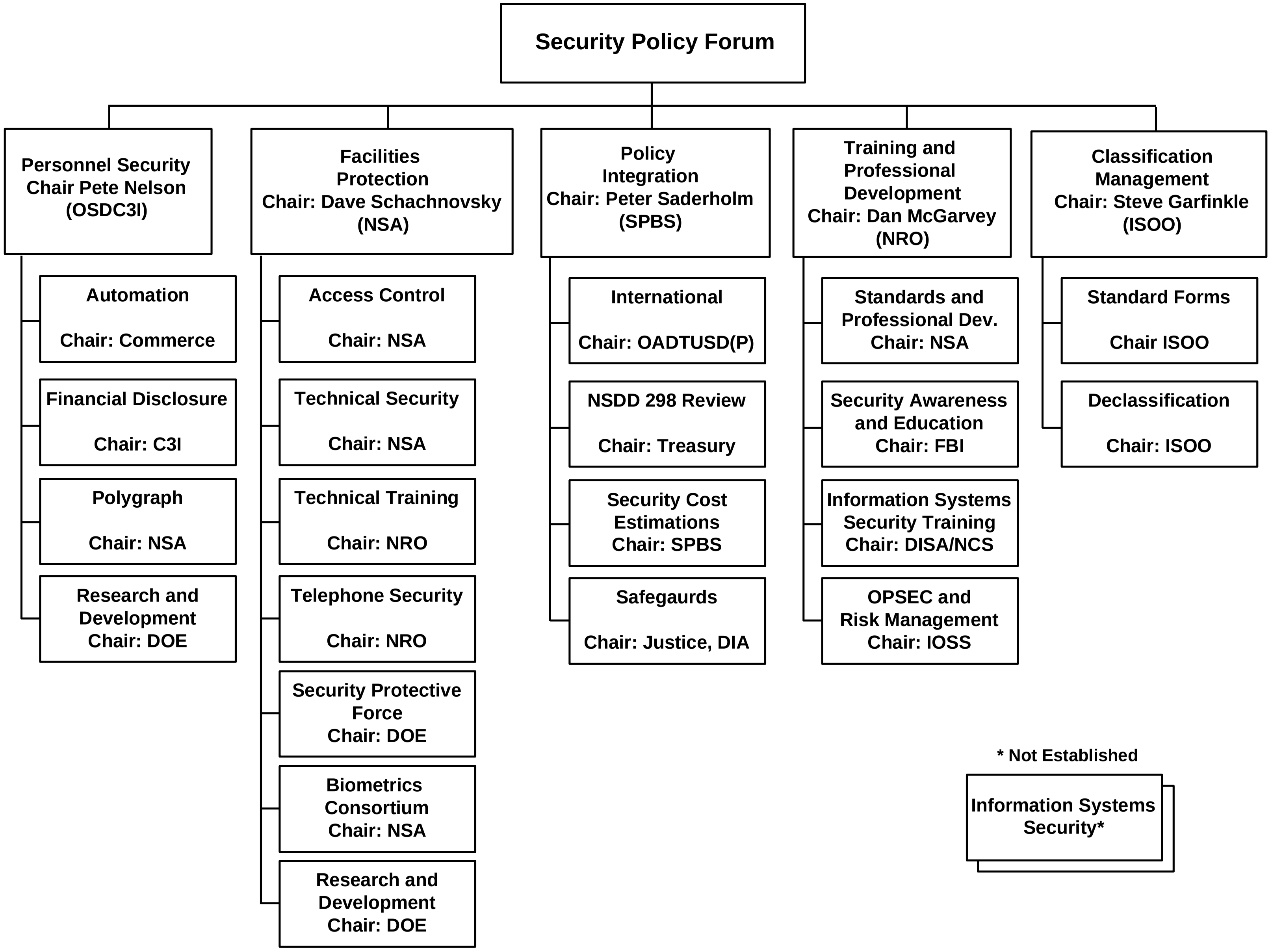
  - The National Counterintelligence Policy Board established by PDD-24, the Security Policy Board, and the Overseas Security Policy Board, will coordinate as necessary on policy issues that may be of mutual concern, and each Board will implement procedures for such coordination. Conflicts between these Boards that cannot be resolved will be referred to the Principals Committee of the National Security Council. The Chairman of these Boards will meet at least on an annual basis to review policy coordination.
  - The Security Policy Board, Forum, and any interagency working groups established by these bodies will be supported by a Staff which will operate under the direction of the Security Policy Board. This Staff will also provide administrative and personnel support to the Security Policy Advisory Board, which will operate independent of other Staff functions and personnel under the direction of the Chairman of this Advisory Board. Staff personnel will be provided or funded by the member agencies of the Security Policy Board.

- During its first year, the Board, with its substructure of the Security Policy Forum (Forum), five standing committees, and ad hoc working groups, all regularly kept informed by key industrial representatives, has served to facilitate reciprocity and commonality by engaging 27 federal agencies and departments in the dialogue and process that lead to national policy formulation. The Board, composed of 10 deputy secretaries or under secretaries or equivalent, functions primarily to rule on policies formulated by the Forum and standing committees and, when required, resolve conflicts that arise the substructures, Such a high-level conflict resolution mechanism was unheard of in previous attempts to organize the U.S. Government security structure. The process of policy development now moves at a much quicker speed and enjoys government-wide “buy-in” by member agencies and departments.

- The process of streamlining policy development could not be accomplished without first reducing and revamping the security policy structures that operated within the government. Once there were eight organizations for developing policy relating to the protection of facilities; we now have the Overseas Security Policy Board responsible for the overseas facilities such as U.S. embassies and consulates that under the Chief of Missions, and the Board responsible for all other aspects of U.S. security policy. Once there were two personnel security policy organizations, there is now one. There has never been a government-wide organization with the mission to standardize, professionalize, and modernize security training and professional development within the government; there is now one. The information Security Oversight Office (ISOO) and Classification Management Committee (CMC) of the Board have forged a close partnership to reform classification and safeguarding procedures. A Policy Integration Committee has been established to focus on overarching issues such as security costs and risk management as well as the eradication of redundancy among similar security programs. Close liaison and cooperative efforts have been established with the Overseas Security Policy Board, the National Counterintelligence Policy Board and the National Counterintelligence Center.

Consultations with these organizations occur as warranted during the policy development process.

- The Board and is subordinate structure has adopted the findings of the JSC to serve as the initial blueprint for needed reform During 1995, the Board has completed 20 percent of the 76 recommendations from the JSC. In total, the Board is currently addressing 114 distinct actions encompassing a wide range of security issues and priorities.
- The greatest challenge to confront the Board has been in the area of information systems security. The Board found well-intentioned, but fragmented groups, committees, panels, and boards, each trying to deal with some particular aspect or subset of Information Systems Security and closely-related Defensive Information Warfare. Recently, the Board Staff and the senior leadership of the Information Infrastructure Task Force Security Issues Forum, began sponsoring a series of meetings between representatives of the Civil and DoD/Intelligence Communities. The goal of these meetings is to advance mutual understanding of the topic, identify commonalties between the classified and unclassified systems and their vulnerabilities, and to come to an agreement on the these issues are to be addressed..
- The Board and its underlying committee structure has made significant strides in eliminating the fragmentation that exists in the security policy of the nation. By mobilizing 27 federal agencies and departments, with industry's advice and counsel, unified policy is being developed that:
    - is based on sound risk management;
    - is in consonance with the overall goals established in PDD-25;
    - takes into account the diverse threats our nation now faces, and;
    - recognizes a renewed interest and respect for the public's right to know.


Security Policy Forum
Personnel Security
Chair Pete Nelson
(OSDC3I)
Automation
Chair: Commerce
Financial Disclosure
Chair: C3I
Polygraph
Chair: NSA
Research and
Development
Chair: DOE
Facilities
Protection
Chair: Dave Schachnovsky
(NSA)
Access Control
Chair: NSA
Technical Security
Chair: NSA
Technical Training
Chair: NRO
Telephone Security
Chair: NRO
Security Protective
Force
Chair: DOE
Biometrics
Consortium
Chair: NSA
Research and
Development
Chair: DOE
Policy
Integration
Chair: Peter Saderholm
(SPBS)
International
Chair: OADTUSD(P)
NSDD 298 Review
Chair: Treasury
Security Cost
Estimations
Chair: SPBS
Safegaurds
Chair: Justice, DIA
Training and
Professional
Development
Chair: Dan McGarvey
(NRO)
Standards and
Professional Dev.
Chair: NSA
Security Awareness
and Education
Chair: FBI
Information Systems
Security Training
Chair: DISA/NCS
OPSEC and
Risk Management
Chair: IOSS
Classification
Management
Chair: Steve Garfinkle
(ISOO)
Standard Forms
Chair ISOO
Declassification
Chair: ISOO
* Not Established
Information Systems
Security*

United States Security Policy Board

Information Assurance Document Review Group

Organization: Security Policy Board Information Assurance Document (SPB IAD) Review Group/Working Group

Senior Information Warfare Official:

Peter D. Saderholm, Director, USSPB Staff

Information Warfare Points of Contact:

Vicki A. LaBarre, USSPB Staff

On-Line Resources:

Information Warfare Related Missions and Functions:

The Director of the US Security Policy Board Staff committed to the production of the Security Policy Board Information Assurance Document (IAD) No. 1 within the first six months of calendar year 1996. This document will be an attempt to provide requirements to assure the confidentiality, availability, and integrity of information systems. Industry's counsel on this matter is considered critical and, they are being included in the dialogue. The Director initiated the development of this document by the Staff due to absence of a standing committee concerned with the security of information systems reporting to the Forum,

The proposed INFOSEC policy under development by this working group will attempt to address INFOSEC in an innovative manner by encompassing the changing security and properties of data as it moves through networks, from system to system, through all of its states of transmission, processing, and storage.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- On 29 March 1966, the Drafting Group successfully concluded the first draft of IAD No. 1. The draft was presented to the Review Group which includes representatives from all 27 departments/agencies/military services, as well as industry. Subsequent draft and reviews will be based on the perceived acceptability and utility of the document. As far as practical, every question brought up by the Review Group will be answered by the Drafting Group, either by inclusion in the next draft or by written reply. The goal is to provide, by early summer 1996, a completed and coordinated document for review by the Security Policy Forum.

This page intentionally left blank.

Advisory Committees

Advisory Committees

This page intentionally left blank.

Committee of Advisors on Science and Technology

Organization: Committee of Advisors on Science and Technology

Senior Information Assurance Official:

Information Assurance Points of Contact:

On-Line Resources:

Committee Homepage: http://www.whitehouse.gov/WH/EOP/OSTP/NSTC/html/pcas.html

Information Assurance Related Missions and Functions:

President Clinton established the President's Committee of Advisors on Science and Technology (PCAST) by Executive Order 12882 at the same time that he established the NSTC. The PCAST serves as the highest level private sector advisory group for the President and for the NSTC. The Committee members are distinguished individuals appointed by the President, and are drawn from industry, education and research institutions, and other non-governmental organizations. The Assistant to the President for Science and Technology co-chair the Committee with a private sector member selected by the President.

The formal link between the PCAST and the NSTC ensures that national needs remain an overarching guide for the NSTC. The PCAST provides feedback about Federal programs and actively advises the NSTC about science and technology issues of national importance.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

Computer System Security and Privacy Advisory Board

Organization: Computer System Security and Privacy Advisory Board

Senior Information Assurance Official:

Dr. Willis Ware, Chairman, RAND

Information Assurance Points of Contact:

Ed Roback, Board Secretary, National Institute for Standards and Technology

On-Line Resources:

CSSPAB Homepage: http://crsc.nist.gov/csspab

Information Assurance Related Missions and Functions:

In accordance with the requirements of Section 3 of the Computer Security Act of 1987 (P.L. 100-235), the Secretary of Commerce established the Computer System Security and Privacy Advisory Board, pursuant to the Federal Advisory Committee Act.

The Computer Security Act specifies that the Board's mission is to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy.

The Board examines those issues affecting the security and privacy of sensitive unclassified information in federal computer and telecommunications systems. The Board's authority does not extend to private-sector systems or federal systems which process classified information.

The Board advises the Secretary of Commerce and the Director of the National Institute of Standards and Technology (NIST) on computer security and privacy issues pertaining to sensitive unclassified federal computer systems. The Board reports its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and appropriate committees of Congress.

NIST personnel serve as the Board's Secretariat. Other federal agency personnel may also assist the Board's activities as specified in the Computer Security Act of 1987.

The membership of the board includes: four members outside the Federal government eminent in the computer or telecommunications industry, including at least one representative of small or medium sized companies in such industries; four members from outside the Federal government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed or representatives of a producer of computer or telecommunications equipment; and four members from the Federal government, including one from the National Security Agency, who have computer systems management experience, including experience in computer systems security and privacy.

The Board reports through the Director of the National Institute of Standards and Technology to the Secretary of Commerce, and as required by Section 3 of the Computer Security Act of 1987, to the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate committees of the Congress. Members include:

Dr. Willis Ware (Chairman)
Computer Research Staff
RAND

Mr. Charlie Baggett
National Security Agency

Ms. Genevieve Burns
American Express Travel Related Services Company, Inc.

Mr. Addison Fischer
Fischer International Systems Corporation

Ms. Sandra Lambert
Lambert and Associates

Mr. Joseph Leo
U.S. Department of Agriculture

Ms. Gloria Parker
Department of Education

Mr. Randolph Sanovic

Mr. George Spix
Microsoft Corporation

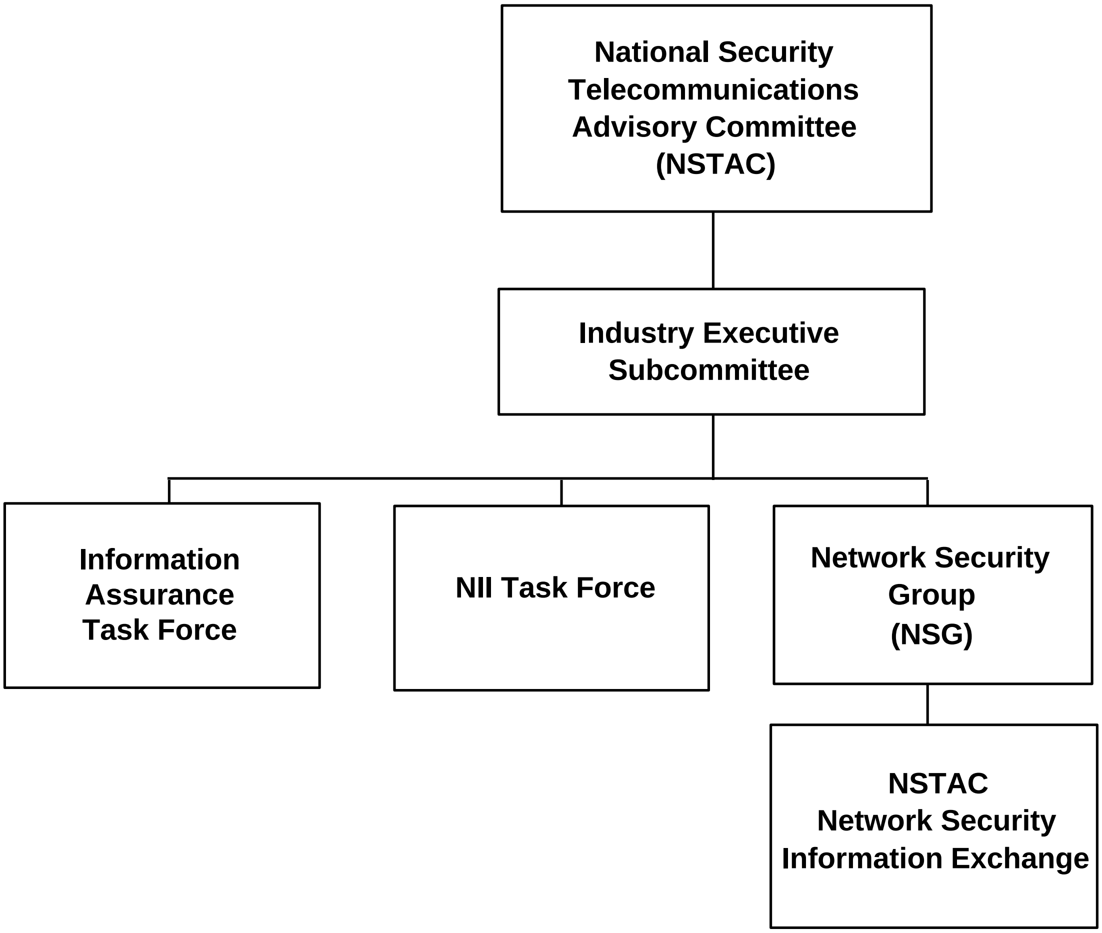
Ms. Linda Vetter

Mr. Frederick Weingarten
Computing Research Association

Mr. Bill Whitehurst
International Business Machines Corporation

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Board meets three to four times per year. The Board receives extensive updates and comments on on-going security and privacy activities throughout the Federal government and the private sector. The Board has been focusing on the following topics:
  - Encryption legislation and policy
  - Encryption products (government and commercial)
  - Key escrow
  - Common criteria for information technology security evaluation
  - Emerging security policy and implementation (e.g., Revised Appendix III to OMB Circular A-130)
  - Computer security lessons learned


National Security Telecommunications Advisory Committee (NSTAC)
Industry Executive Subcommittee
Information Assurance Task Force
NII Task Force
Network Security Group (NSG)
NSTAC Network Security Information Exchange

Organization: National Security Telecommunications Advisory Committee

Senior Information Assurance Official:

Information Assurance Points of Contact:

Fred Herr, Office of the Manager, National Communications Systems

On-Line Resources:

NSTAC Homepage: http://164.117.147.223/~ncs/html/nstac.html

Information Assurance Related Organizations, Missions and Functions:

E.O. 12382 established the President's National Security Telecommunications Advisory Committee (NSTAC) to provide advice and information from the perspective of industry to the President and the Executive Branch with respect to national security telecommunications policy and enhancements to NS/EP telecommunications.

Current NSTAC members are:

- ATCD
- AT&T Corporation
- Bank of America
- Bell Communications Research, Incorporated
- The Boeing Company
- Communications Satellite Corporation
- Computer Sciences Corporation
- CST
- Electronic Data Systems
- GTE Corporation
- Hughes Aircraft Company
- International Business Machines Corporation
- Interdigital
- ITT Corporation
- Lockheed-Martin
- Loral Corporation
- MCI Communications Corporation
- MFS Communications Company, Inc.
- Motorola, Incorporated
- Northern Telecom, Incorporated
- Pacific Telecom, Incorporated
- Rockwell International Corporation
- Science Applications International Corporation
- Sprint Corporation
- Teledisic
- TRW, Incorporated
- Unisys Corporation
- Telephone Association
- West, Incorporated
- WorldCom

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

Wireless Services Task Force (WSTF)

- The WSTF is charged with:
    - Supporting Federal government efforts to implement Cellular Priority Access Service (CPAS). Provide advice, assist in dealing with standards and other industry bodies, support CPAS implementation activities with users and service providers, and participate in joint meetings. (CPAS would provide call-by-call priority access service for cellular radio.)
    - Determining the NS/EP implications and identifying the future task force involvement in the following emerging wireless systems and report to IES:
        - Land Mobile Radio/Specialized Mobile Radio (LMR/SMR)
        - Mobile Satellite Services (MSS)
        - Personal Communications Services (PCS)
        - Mobile Wireless Access to Data Networks
- The WSTF issued an Emerging Wireless Services Report. The report concluded that:
    - NS/EP telecommunications capabilities could benefit from a joint industry-government investigation of the use of new wireless technologies in NS/EP operations.
    - It would be beneficial for Federal, State, and local representatives to collaborate on NS/EP issues involved in new and evolving wireless technologies.
- In addition, the report recommended that the Government should:
    - Define and establish unified policies and requirements for wireless services in support of NS/EP activities at Federal, State and local levels.
    - Identify NS/EP issues inherent in emerging technologies to include providing NS/EP orientation to newly involved entities.
    - Identify interoperability and security constraints inherent in emerging wireless technologies and determine alternative solutions.
    - Identify approaches to providing end-to-end network privileges for NS/EP users associated with these new technologies.

NII Task Force

- The NII Task Force was established in August 1993 to provide the President guidance on the types of government policies, programs, and applications that should be implemented to ensure N/SEP requirements are satisfied in the evolving NII.
- Most recently the NII Task Force has addressed three charges from NSTAC XVII:
    - Determine the need for and, if found appropriate, develop a proposed charter for an NII Security Center of Excellence (SCOE)
    - Determine the NS/EP implications of the emerging global information infrastructure (GII)
    - Complete a current assessment and report on emergency health care information issues.

- With regard to these charges the NII Task Force concluded that:
  - A national level organization (SCOE) is needed to address unmet NII security functions: adoption of security evaluation standards and techniques; coordination in the development of standards; development and promulgation of methodologies for testing and rating security products and services; education of private, corporate, organizational and government users, providers, and decision makers.
  - Furthermore, the SCOE model should be private sector-based, privately funded, and include users, providers, professional associations, and vendors. Also, an Information Systems Security Board (ISSB), based on the Financial Accounting Standards Board (FASB) model, could perform the security functions identified by the task force.
  - The U.S. Government, in conjunction with other governments and U.S. telecommunications and information industries, should continue to define, sponsor, and participate in international projects that raise technology and policy issues critical to the evolution of the GII.
  - The IES, in cooperation with the U.S. Government, should address the increasing NS/EP threat to the NII resulting from the evolving GII.
  - With regards to Emergency Health Care Information, the President should urgently ensure that ongoing activities (e.g., those in response to PDD 39) are coordinated to do the following:
    - Develop and maintain integrated plans, including emergency communications, to ensure that existing and evolving NII capabilities can support a coordinated emergency medical response to nuclear/biological/chemical incidents or similarly catastrophic events.
    - Regularly exercise and evaluate response plans.
    - Identify and examine other critical response infrastructures to determine if the emergency communications and information management issues found with emergency medical response are shared.
    - Actively involve NSTAC in the review of the coordinated emergency plans.

Network Security Group

- The Network Security Group is charged with the following responsibilities:
  - Oversee NSTAC Network Security Information Exchange (NSIE)
  - Represent NSTAC on network security matters to the Manager, NCS, and the FCC’s Network Reliability Council.
  - Participate in the research and development information exchange between government and industry.
- Recently, the Network Security Group has explored the concept of “middle-ground” security that should provide sufficient protection for the corporate and individual users while balancing the needs of the law enforcement and intelligence communities.

- Conducted NSIE Risk Assessment focusing on current and near-term public networks. The report concluded that:
  - Reliance on Public Networks is increasing.
  - Explosive growth of new types of service providers and new technology is increasing the complexity of the network and its interfaces, introducing new vulnerabilities.
  - Deterrent capabilities are improving, but have not kept pace with the threat.
  - Protection measures are improving, but have not kept pace with the vulnerabilities.
  - Risk to public networks is greater today than reported in 1993.
- Furthermore, the NSG Perspective on Risk notes that:
  - Current Federal computer crime laws are not fully effective.
  - Government and industry sponsored R&D is insufficient.
  - Nationwide indications, warnings and assessment capability does not exist.

Information Assurance Task Force

- The Information Assurance Task Force is conducting a Risk Assessment of the following infrastructures:
  - Electric generation, transmission, and distribution system (estimated completion date: fall 1996)
  - Financial system (estimated completion date: end 1997)
  - Transportation system (tentative completion date: summer 1997)

This page intentionally left blank.

Network Reliability and Interoperability Council

Organization: Network Reliability and Interoperability Council (NRIC)

Senior Information Assurance Official:

Information Assurance Points of Contact:

On-Line Resources:

Information Assurance Related Organizations, Missions and Functions:

The Network Reliability and Interoperability Council (NRIC) is a Federal Advisory Committee chartered by the Federal Communications Commission (FCC). The charter was renewed for a third two-year term beginning January 6, 1996. This advisory committee was first chartered in the spring of 1992 to investigate reliability of the public switched network after several service outages during 1990 and 1991 affected large numbers of users and an air traffic control system. During its first two terms the committee, then named the Network Reliability Council (NRC), recommended a system for common carrier reports to the FCC when service outages affect either a large number of users or critical facilities, such as major airports and important government locations. Implementation of reporting was expedited by using a voluntary process and was finalized by adoption of an FCC rule. [47 C.F.R. 63.100]

Members of the Council include Chief Executive Officers and other executives of major telecommunications common carriers, equipment suppliers, communications trade associations, research facilities, standards organizations, cable companies, computer industry firms, satellite companies, consumer organizations, communications employees, state regulators, and Federal government user representatives. Subordinate focus groups operate within an industry standards organization, the Alliance for Telecommunications Industry Solutions (ATIS), under the direction of the Network Reliability Steering Committee (NRSC). The focus groups are as follows:

Performance Metrics Team
Best Practices Team
Outage Reporting and Customer Notification Team
Increased Interconnection Task Group
Reliability Issues - Changing Technologies Focus Group:
- SONET/ATM
- New Wireless Technologies
- Satellite Communications Networks
- Wireless/PCS
- Advanced Intelligent Network
- Essential Communications During Emergencies
- Telecommuting as a Back-up in Emergencies

In June 1993 the Council published an extensive report of its work, “Network Reliability: A Report to the Nation,” in fulfillment of its original charter and mission. Council findings had proven to be an effective basis for improvement of network reliability in the industry. It was therefor important to ensure that a broadly based committee of industry experts remained actively involved in further reducing the number of outages and their effect on users.

In renewing the charter for a second two year term, effective July 1994, the FCC requested the Council to: (1) evaluate the reliability of network services on a local and regional basis, (2) evaluate potential risks from new interconnection arrangements, (3) assess the impact of changing technologies including cable television and wireless, (4) evaluate access to emergency services during network outages, and (5) determine whether network outages have disproportionate impact on certain geographic areas or certain demographic groups. These functions continue into the following charter period.

A new charter, effective January 6, 1996, continues the Council during this era of deregulation, increasing competition, and rapid technological change. The Telecommunications Act of 1996, effective February 8, 1996, is a major revision of the Communications Act of 1934. The changes favor competition between existing telecommunications common carriers without geographic or territorial market distinctions. Competitive entry to the market is also eased for non-traditional providers including power, computer, railroad, cable television, satellite, and pipeline companies. The 1996 Act provides a legislative basis for Open Network Architecture (ONA) which is the unbundling of network and switched service elements. Existing FCC rules had established ONA, primarily to enable competitive access providers to interconnect their services to users through facilities of local exchange carriers. The 1996 Act includes requirements for all carriers to cooperate in ensuring interoperability of their services.

Members of the NRIC include:

Interexchange Carriers

AT&T
MCI Comm. Corp.
Sprint

Local Exchange Carriers
Ameritech
Bell Atlantic
Bell South
GTE Corporation
NYNEX Corporation
Pacific Telesis
Southwestern Bell
US West, Inc.
Rochester Telephone

Research and Standards Groups

Bell Communications Research (Bellcore)
Alliance for Telecommunications Industry Solutions (ATIS)
Cox Cable Communications, Inc. (Cable Labs)

Trade Associations

Association for Local Telecommunications Services (ALTS)
Competitive Telecommunications Association (COMPTEL)
Organization for the Protection and Advancement of Small Telephone Companies (PASTCO)
United States Telephone Association (USTA)
Telecommunications Industry Association (TIA)
National Cable Television Association (NCTA)
Cable Telecommunications Association (CATA)
Personal Communications Industry Association (PCIA)
Cellular Telecommunications Industry Association (CTIA)

Large Consumer Representatives

Ad Hoc Telecommunications Users Group
International Communications Association (ICA)

Small Consumer Representatives

Alliance for Public Technology
National Association of State Utilities Consumer Advocates (NASUCA)

Cable Companies

Time Warner Communications

Satellite Representatives

Hughes Space and Communications Company

Government Related Organizations

National Association of Regulatory Utility Commissioners (NARUC)
National Communications System

Labor

Communications Workers of America, AFL-CIO

Computer Firms

IBM

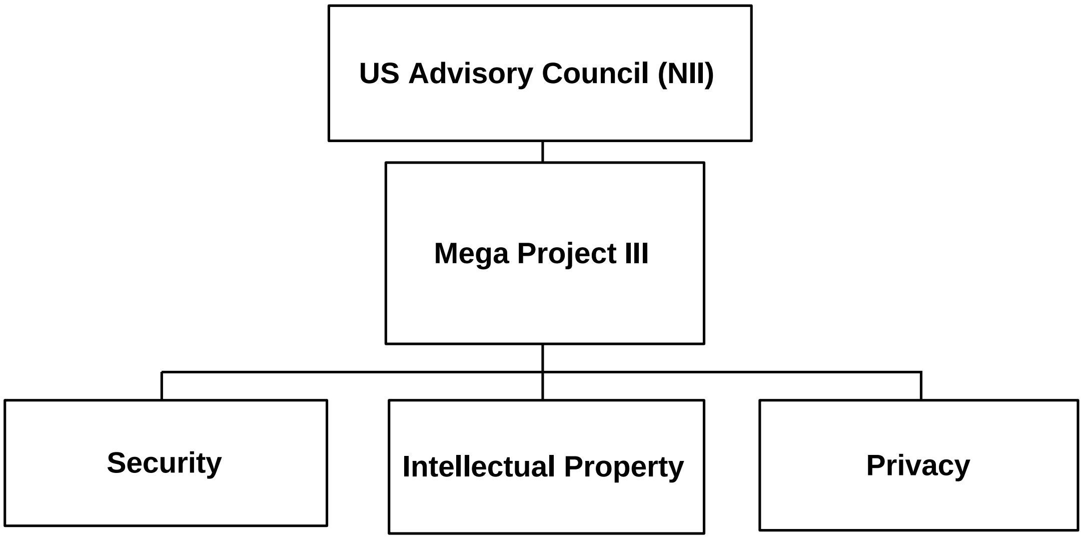
Observer Members

National Telecommunications and Information Administration, U.S. Department of Commerce

Office of Science and Technology Policy, White House

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

This page intentionally left blank.


US Advisory Council (NII)
Mega Project III
Security
Intellectual Property
Privacy

Organization: United States Advisory Council on the NII

Senior Information Assurance Official:

N/A

Information Assurance Points of Contact:

Yvette Barrett, IITF Secretariat

On-Line Resources:

USAC Homepage: http://niiac-info.org/~niiac

Information Assurance Related Organizations, Missions and Functions:

Established by Executive Order No. 12864, the Advisory Council on the National Information Infrastructure (NII) was established to identify appropriate government action and advise the Secretary of Commerce, on matters related to the development of the NII. The Council members represented the many different stakeholders in the NII, including industry, labor, academic, public interest groups, and state and local governments.

Current members are:

Mr. Morton Bahr, President
Communications Workers of America, AFL-CIO
Dr. Toni Carbo Bearman, Dean and Professor,
School of Library and Information Science University of Pittsburgh
Ms. Marilyn Bergman
President, American Society of Composers, Authors, and Publishers (ASCAP)
Ms. Bonnie Laverne Bracey, Teacher
Ashlawn Elementary School, Arlington, Virginia
Mr. John F. Cooke, President
The Disney Channel
Ms. Esther Dyson, President
EDventure Holdings
Mr. William C. Ferguson, Chairman and Chief Executive Officer
NYNEX corporation
Dr. Craig Fields, Chairman and Chief Executive Officer
Microelectronics and Computer Technology Corporation
Mr. Jack Fishman, Publisher
Citizen-Tribune
Ms. Lynn Forester, President and Chief Executive Officer
Firstmark Holdings, Inc.

Honorable Carol Fukunaga, Senator
State of Hawaii
Mr. Jack Golodner, President
Department for Professional Employees, AFL-CIO
Mr. Eduardo Gomez, President and General Manager
KABQ Radio, Albuquerque, New Mexico
Mr. Haynes G. Griffin, President and Chief Executive Officer
Vanguard Cellular Systems, Inc.
Dr. George Heilmeier, President and Chief Executive Officer
Bellcore (Bell Communications Research)
Ms. LaDonna Harris, President
Americans for Indian Opportunity
Ms. Susan Herman, General Manager
Department of Telecommunications, City of Los Angeles
Mr. James R. Houghton, Chairman and Chief Executive Officer
Coming Incorporated
Mr. Stanley S. Hubbard, Chairman and Chief Executive Officer
Hubbard Broadcasting, Inc. and the United States Satellite Broadcasting Company, Inc.
Mr. Robert L. Johnson, Founder and President
Black Entertainment Television (BET)
Dr. Robert E. Kahn, President
Corporation for National Research Initiatives (CNRI)
Ms. Deborah Kaplan, Vice President
World Institute on Disability
Mr. Mitchell Kapor, Chairman
Electronic Frontier Foundation
Mr. Delano E. Lewis, President and Chief Executive Officer
National Public Radio (NPR)
Mr. Alex J. Mandl, Chief Executive Officer
Communications Services Group, AT&T
Mr. Edward R. McCracken, Chairman and Chief Executive Officer
Silicon Graphics, Inc.
Dr. Nathan Myhrvold, Senior Vice President of Advanced Technology
Microsoft Corporation
Mr. N.M. (Mac) Norton, Jr., Attorney-at-Law
Wright, Lindsey & Jennings
Mr. Vance K. Opperman, President
West Publishing Company
Ms. Jane Smith Patterson, Advisor to the Governor of North Carolina
for Policy, Budget and Technology
Ms. Frances W. Preston, President and Chief Executive Officer
Broadcast Music Incorporated (BMI)
Mr. Bert C. Roberts, Jr., Chairman and Chief Executive Officer
MCI Communications Corporation

Mr. John Sculley, Former Chairman
Apple Computers, Inc.
Ms. Joan H. Smith, Chairman
Oregon Public Utility Commission
Mr. Al Teller, Chairman and Chief Executive Officer,
MCA Music Entertainment Group
Mr. Lawrence Tisch, President and
Chief Executive Officer, CBS, Incorporated
Mr. Jack Valenti, Chief Executive Officer and President
Motion Picture Association of America

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- In January 1996, the Council issued its final report entitled "A Nation of Opportunity: Realizing the Promise of the Information Superhighway" and officially disbanded. Relevant highlights from the Council's report are extracted below.
  - "The United States stands today in the midst of one of the great revolutions in recorded history: the Information Age. The Information Superhighway provides the infrastructure that enables enormous benefits in education, economic well-being, and quality of life."
  - "Electronic Commerce. The Federal government, in conjunction with others, should take the steps to identify and resolve, wherever possible, legal, regulatory, and policy issues that would restrict the development of electronic commerce on the Information Superhighway."
  - "The Federal government should convene a broad-based committee composed of those entities involved in standard setting, those involved with the development of new technology, and relevant State, local, and Tribal agencies to meet the needs of the emergency management, public safety, and criminal justice communities."
  - "The Federal government should encourage private sector awareness of security issues, initiate a public-private security consultation process, and foster mechanisms to promote private accountability for proper use of security measures."
  - "The Federal government should not inhibit the development and deployment of encryption by the private sector."

This page intentionally left blank.

Independent Establishments and Government Corporations

Independent Establishments and Government Corporations

This page intentionally left blank.

Central Intelligence Agency
J. Deutch

Organization: Central Intelligence Agency

Senior Information Warfare Official:

John Deutch, Director of Central Intelligence
RADM Dennis Blair, Associate Director of Central Intelligence for Military Support

Information Warfare Points of Contact:

Chief, Critical Defense Technologies Division, Office of Weapons, Technology, and Proliferation
Chief, Information Warfare Brranch (CTD, OWTP)

On-Line Resources:

CIA Homepage: http://www.odci.gov/cia/

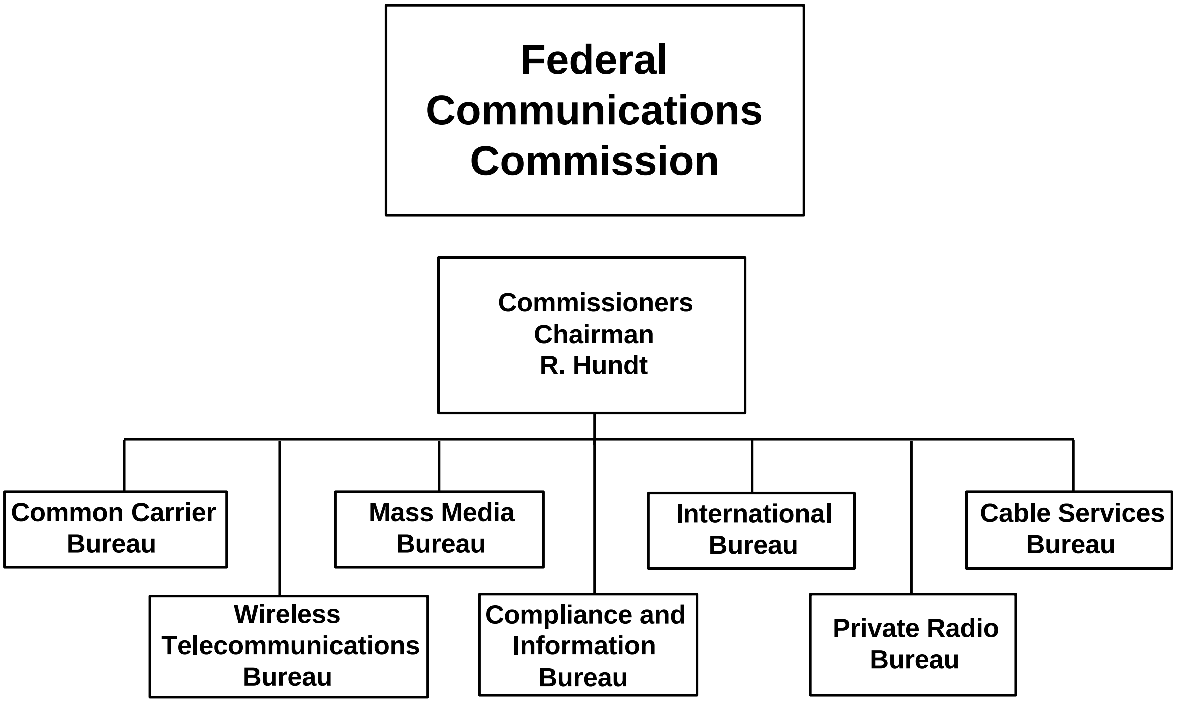
Information Warfare Related Missions and Functions:

Overall policy and tasking for the Intelligence Community in general, and for the CIA in particular, to supply foreign intelligence support to the U.S. government on information warfare issues and activities.

The Office of Weapons, Technology, and Proliferation (OWTP) focuses on scientific and technical intelligence on foreign military R&D and system development and acquisition. The Critical Defense Technologies Division has been tasked with looking at new technology development and related acquisition programs for information system technologies, inter alia.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- This is a relatively new thrust for the Intelligence Community, and they have just begun to adjust to deal with this “new” warfare area.


Federal Communications Commission
Commissioners Chairman R. Hundt
Common Carrier Bureau
Mass Media Bureau
International Bureau
Cable Services Bureau
Wireless Telecommunications Bureau
Compliance and Information Bureau
Private Radio Bureau

Organization: Federal Communications Commission (FCC)

Senior Information Assurance Official:

Vacant, Defense Commissioner

Information Assurance Points of Contact:

Arlan Van Doorn, Deputy Chief, Compliance and Information Bureau, Representative to the NCS Committee of Principals
Roy Kolly, Compliance and Information Bureau, Representative to the NCS Council of Representatives
Herbert Neumann, Common Carrier Bureau, Representative to the NCS National Coordinating Center for Telecommunications

On-Line Resources:

http://www.fcc.gov/

Information Assurance Related Missions and Functions:

The Federal Communications Commission regulates, licenses and monitors the operation of communications services to ensure reliable and competitive nationwide and international communications. The services regulated include broadcast (radio and television), telephone, wireless (cellular, PCS, satellite), and other digital and analog applications. Transmission facilities include radio, wire, cable, light-guide and satellite. FCC functions include ensuring that communications capabilities are provided for the promotion of life and property and for the national defense.

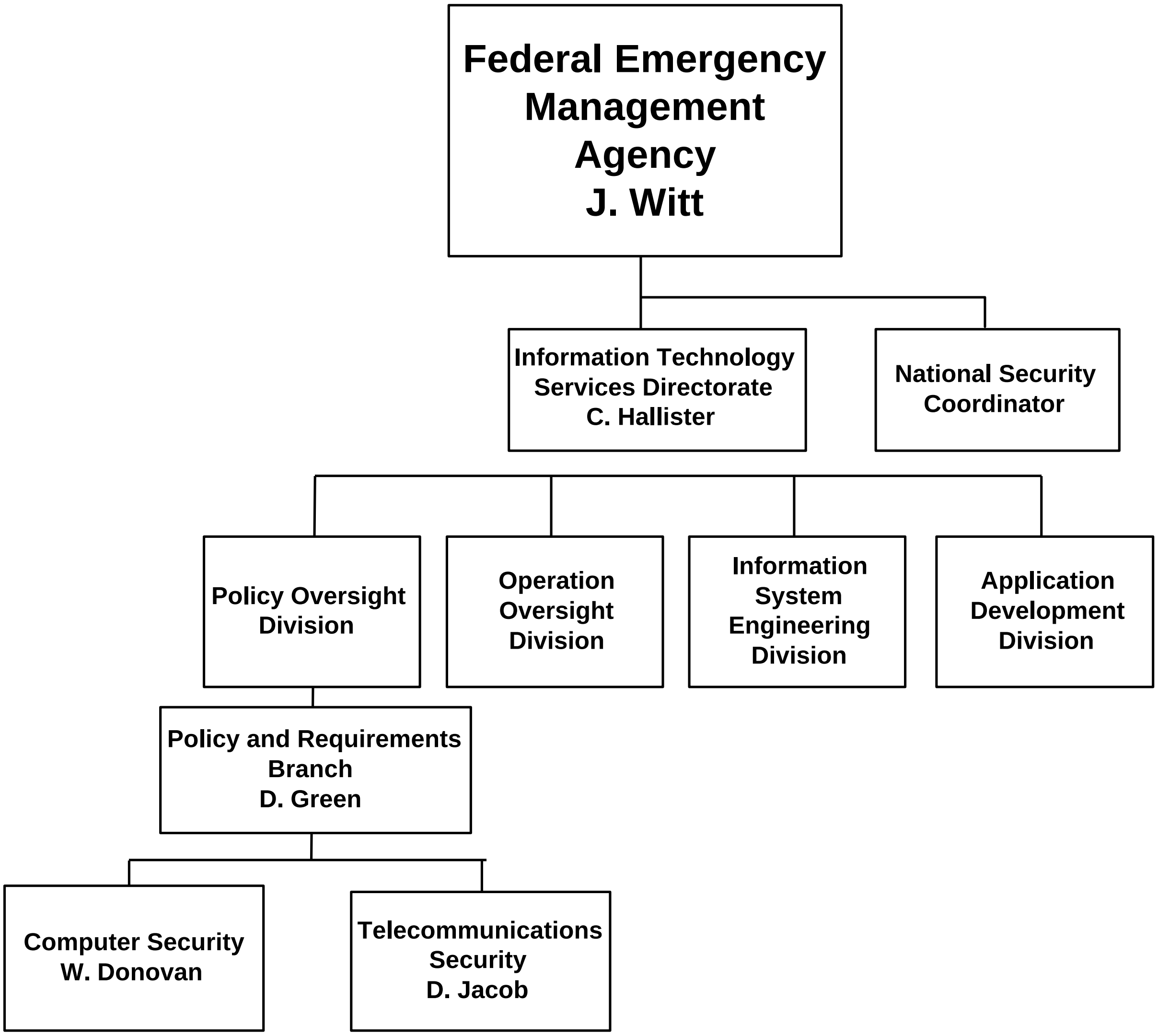
The Commission uses a combination of required reports and its own investigation to monitor performance of licensees. In the telecommunications area, a Federal Advisory Committee, now designated the Network Reliability and Interoperability Council (NRIC), was chartered in 1992 to investigate reliability of the public switched network after the occurrence of several major service outages. The NRIC recommended a system of common carrier reports which the Commission adopted (47 C.F.R. 63.100). Reports are required from any common carriers that experiences a service outage that affects either 30,000 potential users for at least 30 minutes or when an outage impacts a major airport (as defined by the FAA), a major government or military facility, a nuclear power plant, or an emergency 911 tandem switch. Outages involving nuclear power plants, government facilities and military facilities are reported through the NCS National Coordinating Center (NCC). The initial report is made to the DISA Network Management Operations Center which contacts NCC staff members. NCC staff members evaluate the impact and report it to the FCC Watch Officer, if appropriate. Other outages are reported directly to the FCC Watch Officer in Washington, DC. A backup reporting location is also available. Telephonic reports are followed by hard copy reports and final reports are due within 30 days. The telecommunications industry has used the NRIC as an effective vehicle for cooperation in improving network reliability and resiliency. An organizational summary of the NRIC can be found under Advisory Committees in this appendix.

The FCC is required to issue rules to enable implementation of the Telecommunications Act of 1996. This Act, effective February 8, 1996, is a major revision of the Communications Act of 1934. The changes favor competition between existing telecommunications common carriers without geographic or territorial market distinctions. Competitive entry to the market is also eased for non-traditional providers including power, computer, railroad, cable television, satellite, and pipeline companies. The 1996 Act provides a legislative basis for Open Network Architecture (ONA) which is the unbundling of network and switched service elements. Existing FCC rules had established ONA, primarily to enable competitive access providers to interconnect their services to users through facilities of local exchange carriers. The 1996 Act includes requirements for all carriers to cooperate in ensuring interoperability of their services.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The primary concern of the FCC and the common carrier industry is network reliability, rather than security of the information carried.
- Carriers have initiated Mutual Aid Agreements in an effort to reduce the impact of service disruptions.
- Industry standards work may result in greater information security because of the shrinking distinction between network control data and message data.
- Network reliability has been improved through addition of geographically diverse multiple routes; use of improved technology, such as self-healing fiber optic ring architecture; and rapid computer controlled rerouting of large circuit groups around network damage, such as a cable cut.
- FCC is a member of the joint government and industry Network Security Information Exchange (NSIE) whose function is to share sensitive information that can be used to counter illegal use of telecommunications to: (1) disrupt service, (2) commit fraud, (3) gain unauthorized access to computers, (4) commit acts of espionage and, (5) engage in other criminal activities. The NSIE is further discussed in the organizational summary of the NSTAC.

This page intentionally left blank.


Federal Emergency Management Agency J. Witt
Information Technology Services Directorate C. Hallister
National Security Coordinator
Policy Oversight Division
Operation Oversight Division
Information System Engineering Division
Application Development Division
Policy and Requirements Branch D. Green
Computer Security W. Donovan
Telecommunications Security D. Jacob

Organization: Federal Emergency Management Agency (FEMA)

Senior Information Assurance Official:

Clay G. Hollister, Associate Director, Information Technology Services Directorate (ITSD)

Information Assurance Points of Contact:

Dennis B. Green, Chief, Oversight Branch, Policy and Oversight Division, ITSD
William W. Donovan, Information System Security, Oversight Branch, Policy and Oversight Division, ITSD

On-Line Resources:

FEMA Homepage: http://www.fema.gov/

Information Assurance Related Missions and Functions:

The Federal Emergency Management Agency (FEMA) is the central agency within the Federal government for emergency planning, preparedness, mitigation, response, and recovery. FEMA funds emergency programs, offers technical guidance and training, and deploys Federal resources in time of catastrophic disaster. FEMA is also responsible for developing plans to ensure the continuity of the Federal government during national security emergencies, and Federal response to the consequences of major terrorist incidents.

FEMA is an independent federal agency with more than 2,400 full time employees: at FEMA headquarters in Washington, DC, at regional and area offices across the country, at the Mount Weather Emergency Assistance Center, and at the FEMA training center in Emmitsburg, Maryland. FEMA also has nearly 4,000 standby disaster assistance employees who are available to help out after disasters. Often FEMA works in partnership with other organizations that are part of the nation's emergency management system. These partners include state and local emergency management agencies, 27 federal agencies and American Red Cross.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Information Technology Services consolidates most of the information systems development and operational activities from throughout the Agency.
- An unclassified February 28, 1995, NSC memorandum states it is the policy of the Administration to continue the preparedness activities cited in Executive Order 12656, Assignment of Emergency Preparedness Responsibilities, November 23, 1986. It further states that “Natural disasters and other emergencies, which may cause widespread or prolonged disruption of critical Federal government functions, also warrant continued consideration as potential national security challenges” and that responsibilities “involve preparedness for any occurrence, including natural disaster, military attack, technological

emergency or other emergency that seriously degrades or seriously threatens the national security." Finally, the memorandum charges FEMA with preparing "an assessment of the existing continuity of operations and continuity of government programs."

- FEMA information assurance activities are not fully developed because of budget and emphasis on response to natural and man-made disasters.
- Absolutely need an Executive Order to assign responsibilities in this area. Policy must include consequences for not following the policy. Health and Safety analog should be reviewed for possible application to the information area.
- Training and education regarding information assurance should be integrated into other training. In addition, this training should be mandatory. Senior leadership awareness, interest, and support is absolutely required! With size of government and the budget decreasing, we must emphasize awareness.
- Suggested forming a Federal government organization which could provide advice and assistance regarding solutions to security problems. This organization should be centrally funded. NIST currently evaluates products but has restrictions on what information can be released to the government at large.
- Bare-bones internal information security policies are in place. Efforts are underway to improve existing policies.
- Donovan is the lone person responsible for developing and implementing computer security for FEMA.
- The Federal Emergency Management Agency's Federal Response Plan (for Public Law 93-288, as amended) describes FEMA's Concept of Operations to address the consequences of any disaster or emergency situation in which there is a need for Federal response assistance under the authorities of the Stafford Act. It is applicable to natural disasters; technological emergencies involving radiological or hazardous material releases; and other incidents requiring Federal assistance under the Act. The Response Plan describes the basic mechanisms and structures by which the Federal government will mobilize resources and conduct activities to augment State and local response efforts. To facilitate the provision of Federal assistance, the Plan uses a functional approach to group the types of Federal assistance which a State is most likely to need under twelve Emergency Support Functions (ESFs). Each ESF is headed by a primary agency, which has been selected based on its authorities, resources and capabilities in the particular functional area. Other agencies have been designated as support agencies for one or more ESF based on their resources and capabilities to support the functional area. The twelve ESFs serve as the primary mechanism through which Federal response assistance will be provided to assist the State in meeting response requirements in an affected area. Federal assistance will be provided to the affected State under the overall coordination of the Federal Coordinating Officer (FCO) appointed by the Director of FEMA on behalf of the President. Federal assistance provided under P.L. 93-288, as amended, is to supplement State and local government response efforts. ESFs will coordinate with the FCO and the affected State to identify specific response requirements and will provide Federal response assistance based on State-identified priorities. Each ESF will provide resources using its primary and support agency authorities and capabilities, in coordination with other ESFs, to support its missions. ESFs will allocate available resources to each declared State based on priorities identified in conjunction with the State and in coordination with the

FCO. If resources are not available within the declared State, the ESF will seek to provide them from a primary or support agency area or region. If the resource is unavailable from an area or region, the requirement will be forwarded to the appropriate ESF headquarters office for further action. One or more disasters may affect a number of States and regions concurrently. In those instances, the Federal government will conduct multi-State response operations; for each declared State, an FCO will be appointed to coordinate the specific requirements for Federal response and recovery within that State. Under multiple State declarations, ESF departments and agencies will be required to coordinate the provision of resources to support the operations of all of the declared States. The following are the primary agencies for the Emergency Support Function listed:

Emergency Support Function	Primary Agency
1. Transportation	Department of Transportation
2. Communications	National Communications System
3. Public Works and Engineering	U.S. Corps of Engineers (DoD)
4. Firefighting	Forest Service (USDA)
5. Information and Planning	Federal Emergency Management Agency
6. Mass Care	American Red Cross
7. Resource Support	General Services Administration
8. Health and Medical Services	Public Health Service (DHHS)
9. Urban Search and Rescue	Department of Defense
10. Hazardous Materials	Environmental Protection Agency
11. Food	U.S. Department of Agriculture
12. Energy	Department of Energy

Federal Reserve System

Organization: Federal Reserve System (FRS)

Senior Information Assurance Official:

For Federal Reserve Banks:
Clyde H. Farnsworth, Jr., Director, Division of Reserve Bank Operations and Payment Systems

For Board of Governors:
Steven R. Malphrus, Division of Information Resources

Information Assurance Points of Contact:

John H. Parrish, Assistant Director, Division of Reserve Bank Operations and Payment Systems
Kenneth D. Buckley, Manager, Division of Reserve Bank Operations and Payment Systems
Raymond Romero, Project Leader, Division of Reserve Bank Operations and Payment Systems

On-Line Resources:

Federal Reserve Banks: http://www.frbatlanta.org/main/frbsites.htm

Information Assurance Related Missions and Functions:

The Federal Reserve System is the central bank of the United States. It is charged by Congress with responsibility for conducting the nation's monetary policy; supervising and regulating banking institutions; maintaining the stability of the financial system; and providing certain financial services to the U.S. government, financial institutions, and foreign central banks. The Federal Reserve is also responsible for promoting efficiency in payment system practices.

In carrying out these responsibilities, the Federal Reserve executes monetary policy, examines commercial banks, transfers funds and government securities, handles government deposits and debt issues, acts as the lender of last resort, and a wide range of other activities. The System consists of seven parts: the Board of Governors, the twelve Federal Reserve Banks and their twenty-five branches, the Federal Open Market Committee, the Federal Advisory Council, the Consumer Advisory Council, the Thrift Advisory Council, and depository institutions.

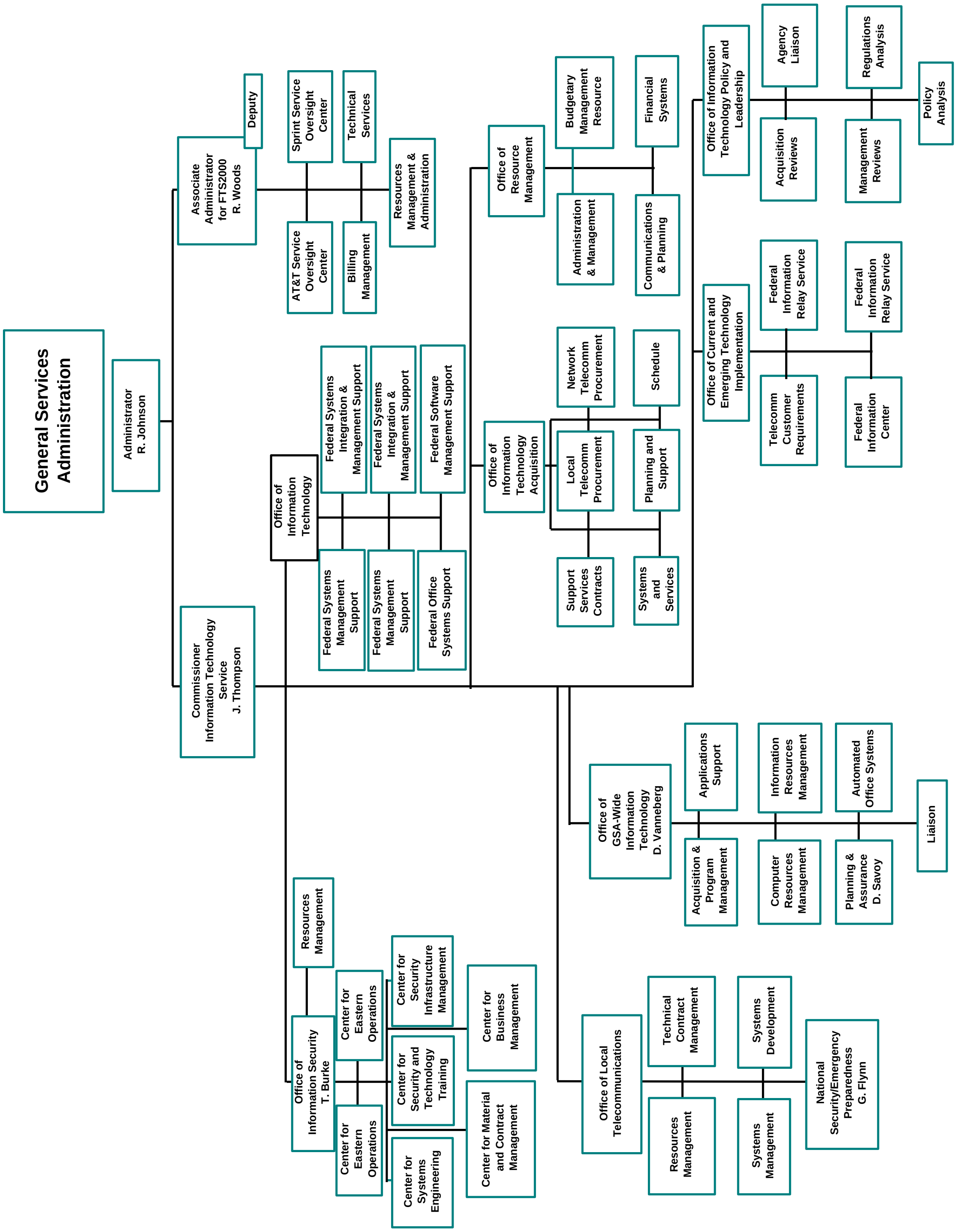
The Board of Governors exercises general supervision over Reserve Bank activities and examines each Reserve Bank annually. The Board approves minimum standards for data security in Reserve Banks, and the effectiveness of the Banks' implementation of controls is evaluated during the annual examinations and during internal audits.

The Board of Directors of each Federal Reserve Bank is composed of nine members: three represent the stockholding member banks and are elected by those banks; three represent commerce, agriculture, or industry in the district and are elected by the stockholding member banks; and three are appointed by the Board of Governors. The Board of Governors appoints one of these latter directors as Chairman of the Board of Directors and another as the Deputy Chairman.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- FRS was created as the Central Bank of the U.S. by act of Congress and is independent within government. Many checks and balances are used to oversee bank operations and maintain the integrity of the System. Parrish's office in the Division of Reserve Bank Operations and Payment Systems is responsible for advising the Board of Governors on the information security aspects of Reserve Bank operations.
- The Chief Operating Officers of each Federal Reserve Bank form a committee to deal with the many aspects of the FRS operation. The committee has in turn formed several working groups to deal with specialized and technical aspects of the FRS operation. One of these working groups is made up of the data security officers of each Federal Reserve Bank. This working group is responsible for developing and recommending security policy. The full committee approves the security policy which is implemented only with the concurrence of the Reserve Bank Operations and Payment Systems, acting on behalf of the Board of Governors.
- Each Federal Reserve Bank conducts internal audits, which include security reviews.
- The Board of Governors examines the Federal Reserve Banks on an annual basis. The Division of Reserve Bank Operations and Payment Systems has oversight responsibility with respect to the security operations of the Federal Reserve Banks.
- Recognition of the public responsibilities of the central bank drive a long-time organizational emphasis on integrity and effective controls in operations. Ownership of and accountability for information, need to know, separation of control, and custody of information procedures have been in place for decades to preserve that integrity. As manual procedures for processing physical valuables were automated over the years, appropriate controls were established for processing in the electronic environment.
- FRS operates three primary data centers and has extensive backup capabilities in the event of partial or whole site failures. Full disaster recovery plans are in place.
- FedWire is the real-time payments system application which provides over $200 trillion in funds transfer and government securities transactions between financial institutions a year. FedNet is the FRS network over which this traffic moves. Fedline is the link between financial institutions and FedWire.
- The Federal Reserve also oversees the Clearing House for Interbank Payments (CHIPS). This is a private sector multilateral net settlement clearing system operated by the New York Clearing House Association in New York City. It clears over $1 trillion a day.

This page intentionally left blank.


General Services Administration
Administrator R. Johnson
Associate Administrator for FTS2000 R. Woods
Deputy
Sprint Service Oversight Center
Technical Services
AT&T Service Oversight Center
Billing Management
Resources Management & Administration
Commissioner Information Technology Service J. Thompson
Office of Information Technology
Federal Systems Integration & Management Support
Federal Systems Integration & Management Support
Federal Software Management Support
Federal Systems Management Support
Federal Systems Management Support
Federal Office Systems Support
Office of Resource Management
Budgetary Management Resource
Financial Systems
Administration & Management
Communications & Planning
Office of Information Technology Acquisition
Network Telecomm Procurement
Schedule
Local Telecomm Procurement
Planning and Support
Support Services Contracts
Systems and Services
Office of Information Technology Policy and Leadership
Agency Liaison
Regulations Analysis
Acquisition Reviews
Management Reviews
Policy Analysis
Office of Current and Emerging Technology Implementation
Federal Information Relay Service
Federal Information Relay Service
Telecomm Customer Requirements
Federal Information Center
Office of GSA-Wide Information Technology D. Vanneberg
Applications Support
Information Resources Management
Automated Office Systems
Acquisition & Program Management
Computer Resources Management
Planning & Assurance D. Savoy
Liaison
Office of Information Security T. Burke
Resources Management
Center for Eastern Operations
Center for Eastern Operations
Center for Security Infrastructure Management
Center for Security and Technology Training
Center for Systems Engineering
Center for Business Management
Center for Material and Contract Management
Office of Local Telecommunications
Technical Contract Management
Systems Development
Resources Management
Systems Management
National Security/Emergency Preparedness G. Flynn

Organization: General Services Administration (GSA)

Senior Information Assurance Official:

Joe M. Thompson, Commissioner, Information Technology Service, GSA

Information Assurance Points of Contact:

Thomas Burke, Deputy Commissioner, Office of Information Security, GSA
G. Flynn, National Security Emergency Preparedness, Office of Local Telecommunications, GSA
R. Woods, Associate Administrator for FTS2000, GSA
D. Venneberg, Deputy Commissioner, Office of GSA-Wide Information Technology, GSA
Diane Savoy, Planning and Assurance Division, Office of GSA-Wide Information Technology, GSA
Bruce Brignall, Post FTS2000 Acquisition Strategy, Office of the Associate Administrator for FTS2000

On-Line Resources:

GSA Homepage: http://www.frbatlanta.org/main/frbsites.htm
GSA Office of Information Security: http://www.gsa.gov/irms/ki/ois.htm
GSA Federal Security Infrastructure: http://www.gsa.gov/fsi/
GSA FSI Civil FORTEZZA Project: http://www.gsa.gov/fsi/fortezza.htm

Information Assurance Related Missions and Functions:

The General Services Administration establishes policy for and provides economical and efficient management of Government property and records, including construction and operation of buildings, procurement and distribution of supplies, utilization and disposal of property; transportation, traffic, and communications management; and management of the Governmentwide automatic data processing resources program. It consists of operating services and support staff offices, with functions carried out at three levels of organization: the central office, regional offices, and field activities.

The Office of Acquisition Policy has a major role in developing, maintaining, issuing, and administering guiding principles via the Federal Acquisition Regulation (FAR) which is applicable to all Federal agencies.

The Office of the Associate Administrator for FTS2000 provides common-user telecommunications and other information services to agencies of the Federal government.

The Information Security Oversight Office is responsible for overseeing executive branch agencies' actions to implement Executive Order 12356, April 2, 1982, which prescribes a uniform system for classifying, declassifying, and safeguarding national security information.

The Office of Information Technology Services provides a variety of services related to information assurance. The office is responsible for coordination and direction of a comprehensive, Government-wide program for the management, procurement, and utilization of automated data processing and local telecommunications equipment and services. The Office of Information Technology Integration provides technical and contracting assistance through three complementary programs: the Federal Systems Integration and Management System (FEDSIM); the Federal Computer Acquisition Center (FEDCAC); and the Federal Information System Support Program (FISSP). The Agency Management Assistance Office conducts several management assistance programs that assist agencies in improving their information-related functions and activities. Among these is the Trail Boss program that helps Federal agencies prepare for major acquisitions. The Information Resources Management Policy Office is responsible for coordinating policy making activities related to information functions and authorities. This office develops, coordinates, and issues Governmentwide automatic data processing and telecommunications acquisition management and use regulations, the Federal Information Resources Management Regulations (FIRMRs). The Information Resources Procurement Office plays a major role in the Governmentwide procurement of automatic data processing and telecommunications hardware, software, and services. In some instances, this office issues a Delegation of Procurement Authority (DPA) which permits Federal agencies to procure their own hardware, software, and services. The Office of Telecommunications Services plays a major role in Governmentwide activities to improve the interagency Information Resources Management (IRM) infrastructure through the Interagency IRM Infrastructure Task Group. This office also manages and administers the National Security Emergency Preparedness Telecommunications Program activities.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

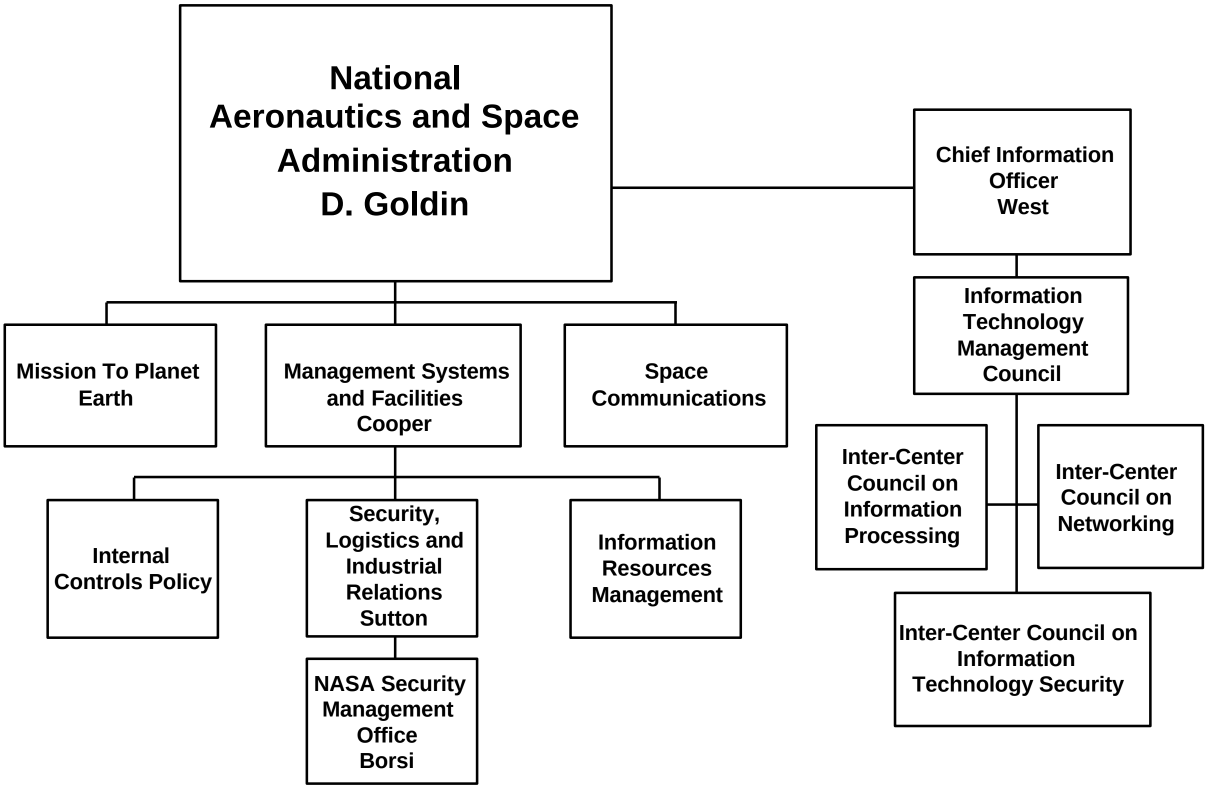
- GSA is involved with infrastructure protection, to include buildings and telecommunications, and works with FEMA and NCS in emergency planning.
- Current objectives are to identify two or three vulnerabilities and to fix them. GSA can not find, fix and react to all security holes, so it must be prudent.
- GSA is planning to encrypt all financial systems in the near future.
- Firewalls and guards are used to protect GSA information and telecommunications and ensure robustness.
- GSA is involved with NSTISSC activities to stand up an infrastructure assurance group, which will coordinate its activities with the Presidential commission.
- A movement towards FORTEZZA is under way that will eventually be implemented in the civil agencies.
- GSA utilizes DOE CERT capabilities for internal assistance. An 800 number has been created that directs calls to the correct incident/emergency response unit.
- Resource reallocation during disruptions of service are managed dynamically by pulled-together teams that draw upon internal assets and expertise.

- GSA released the first draft of a public key encryption policy in April 1996, which is the first step toward establishing government-wide standards for the technology. But the agency must resolve many issues before a final policy can be issued.
- The GSA Office of Information Security was awarded the NSA Rowlett trophy for organizational excellence. GSA's Office of Information Security was recognized for its work in providing technical services to agencies and federal contractors around the globe. The office is also developing security applications for governmentwide electronic commerce and electronic messaging.
- Office of Information Security (OIS) was organized in October 1994, but the services this office provides have been provided by GSA since 1962 beginning with support to the Atomic Energy Commission.
- OIS provides a full spectrum of security services on a reimbursable basis to any customer in the Federal government. The services include engineering, installation, operation and maintenance, systems administration, network management, and a secure packet switching network as a part of FTS 2000. OIS is capable of quick reaction support. The office receives no appropriated moneys. DoD constitutes approximately 60-70 percent of the OIS business and the numbers are growing. Other customers include FBI Legal Attaches, FAA, and the Defense Logistics Agency. These security services support C2, law enforcement operations, regulatory, political, and economic activities, and intelligence operations. OIS also provided coalition warfare support during Desert Shield/Storm and currently supports NATO and UN missions in the Balkans.
- OIS has a long-standing relationship with the National Security Agency (NSA) and the National Institute for Standards and Technology. OIS is currently providing support to the Multilevel Information Systems Security Initiative (MISSI) prototype and to the public key infrastructure prototype. This support includes life-cycle support planning.
- OIS represents GSA in the Information Infrastructure Task Force's (IITF) Security Issues Forum (SIF). OIS participates as a full member in the National Security Telecommunications and Information Systems Security Committee (NSTISSC) and an OIS representative co-chairs, with Treasury, the National Information Infrastructure (NII) Task Force of the NSTISSC. OIS also participates in the Federal Agency Computer Security Program Manager's Forum (FACSPMF). OIS also represents GSA on the Military Communications Electronic Board.
- GSA has three resident program management offices which are chartered by interagency coordinating activities and empowered by agencies and activities having related responsibilities. The offices are the Electronic Commerce Program Management Office (co-chaired by DoD and GSA), the Electronic Mail Program Management Office (chaired by GSA), and the Security Infrastructure Program Management Office which was formed when numerous electronic commerce and electronic mail security issues (such as access control, integrity, non-repudiation, and confidentiality) surfaced. The Electronic Commerce PMO and the Electronic Mail PMO were chartered by the Government Information Technology Services Working Group which supports the Committee on Applications and Technology of the Information Infrastructure Task Force. In addition, the ECPMO was chartered by the Office of Federal Procurement Policy of the Office of Management and Budget. The Security Infrastructure PMO is co-chaired by GSA and

DoD. Intended staffing is approximately 20 people with the staffing being shared among GSA, DISA, NSA, DoJ, Treas, and USPS.

- OIS conducts technical training.
- Issues: Guard technology to allow OIS LAN to interconnect with networks outside the controlled OIS office space.
- Lessons Learned: McAffe network virus checker is identifying viruses other virus checkers should have identified, but did not.
- Information security policy development for GSA is done by the Assurance Division of the Office of GSA-Wide Information Technology. Policy directives in the form of manuals, handbooks, etc. have been published and cover the traditional areas of computer security.
- Brignull operates an interagency group responsible for developing Post FTS2000 acquisition strategy.
- This group is attempting to reach out to the user community to determine needs for Post FTS2000. They have conducted a requirements call and several round tables to address issues such as security and interoperability, wireless services, 800/900 services, data, international, and billing.
- The group seems convinced that there are infrastructure vulnerability problems, but is not sure how to solve them. Possible avenues are legislation, regulation, market forces, and promulgation of industry best practices. Community will also need the help of NIST and NSA.
- The Reliability and Vulnerability Working Group, Telecommunications Policy Committee, Information Infrastructure Task Force, is working on some of the issues. Working group includes has panels working on risk management (chaired by Phil Quaid of NSA), reliability (chaired by Don Nichols of GSA), and standards (chaired by NIST).
- Some of the security and interoperability roundtable issues included warning screens for protected environments, priorities for restoration of services, privacy of billing information, and practicality of standards such as the digital signature standard.
- Of note, cable TV vendors have been added to the FCC’s Network Reliability Council and an international subcommittee has also been added to try to collect international outage information. A recommendation has also been made that a security subcommittee be added.
- The Planning and Assurance Division, Office of GSA-Wide Information Technology, is responsible for writing IT systems security policy for GSA internal operations. The Division recently issued policy guidance on use of Internet. It has also recently distributed through electronic mail a policy directive forbidding the downloading of SATAN. Policy directives are issued in the form of GSA Orders, Memos, and IT Program Updates.

This page intentionally left blank.


National Aeronautics and Space Administration
D. Goldin
Chief Information Officer
West
Information Technology Management Council
Inter-Center Council on Information Processing
Inter-Center Council on Networking
Inter-Center Council on Information Technology Security
Mission To Planet Earth
Management Systems and Facilities
Cooper
Space Communications
Internal Controls Policy
Security, Logistics and Industrial Relations
Sutton
Information Resources Management
NASA Security Management Office
Borsi

Organization: National Aeronautics and Space Administration

Senior Information Assurance Official:

Daniel S. Goldin, Administrator
Ronald S. West, Chief Information Officer
Benita A. Cooper, Associate Administrator for Management Systems and Facilities

Information Assurance Points of Contact:

Russell S. Rice, Director, Information Resources Management Division
Richard W. Carr, NASA Information Technology Security Program Manager
Jeffrey E. Sutton, Director, Security, Logistics, and Industrial Relations Division
Mark J. Borsi, Director, NASA Security Management Office

On-Line Resources:

NASA Homepage: http://www.nasa.gov

Information Assurance Related Missions and Functions:

The National Aeronautics and Space Administration conducts research for the *development of advanced* of problems of flight *designs for aeronautical applications* within and outside the Earth's atmosphere and develops, constructs, tests and operates aeronautical and space vehicles. It conducts activities required for the exploration of space with manned and unmanned vehicles and arranges for the most effective utilization of the scientific and engineering resources of the United States with other nations engaged in aeronautical and space activities for peaceful purposes.

The Office of Mission to Planet Earth conducts NASA's programs that study global climate change and integrated functioning of the Earth as a system. This includes developing and managing remote sensing satellites and instruments, aircraft and ground measurements and research, as well as data and information systems needed to support the objectives of the U.S. Global Change Research Program.

The Office of Space Communications is responsible for meeting requirements critical to NASA's aeronautics and space flight missions. They include spacecraft operations and control centers, ground and space communications, data acquisition and processing, flight dynamics and trajectory analyses, spacecraft tracking and applied research, and development of new technology. A global communications system links tracking sites, control centers, and data processing facilities that provide real-time data processing form mission control, orbit and attitude determination, and routine processing of telemetry data for space missions.

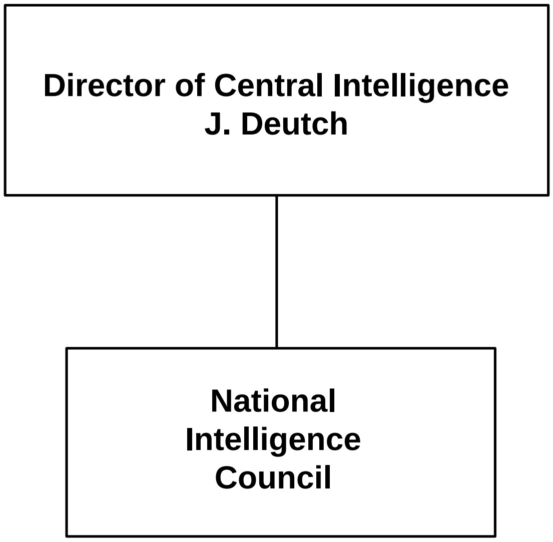
The Goddard Space Flight Center develops and operates information systems technology. The Jet Propulsion Center conducts mission operations and ground based research in information systems technology. The Langley Research Center performs technology experiments in remote sensor and data acquisition and communication technology. The Lewis Research Center conducts research in controls and electronics.

The *NASA CIO* has overall responsibility for information security and information resource management. The NASA Security Management Office is a part of the Security, Logistics and Industrial Relations Division. The Security Management Office is more specifically responsible for policy development and management oversight for *classified information, classified* communications, *classified* automated information, personnel, physical, industrial, and operations security. *Overall corporate-level and Agency-wide functional management* responsibility for Information Technology Security technical integration, implementation, and operation resides in the NASA *CIO* Office.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- NASA has an extensive Information Technology Security program that is integrated into its management functions through management points-of-contact, intra-agency working groups, councils, and committees. The goal of the program is to provide cost-effective protection that assures high integrity ready availability, and confidentiality of NASA automated information resources. The program consists of the following basic elements:
  - Policy and guidance
  - Planning
  - Sensitivity and criticality identification
  - Risk management
  - Protection measures baseline
  - Certifications and re-certifications
  - Self-Assessment *and Compliance assurance*
  - Incident response
  - Awareness and training
- Due to NASA's decentralized approach to managing its *diverse and globally connected* computer and network environments, it has adopted a decentralized approach to implementing its ITS program. NASA headquarters interprets national policy and guidance and issues general policy and guidance internally. Each program office is responsible for establishing an information technology security management function which ensures the security, integrity, and continuity of operations for automated information resources directly related to program missions. Each Center and Data Processing Installation is responsible for establishing and sustaining an information technology security program that assures each data processing center under its management complies with security requirements that are consistent with its mission.
- Each Center is responsible for establishing a Computer (and Network) Security Incident Response (CSIR) capability, which is integrated with the Center's Technical Help Desk facility to provide coverage for local computer systems and local area networks. In addition, NASA has an Agency-wide incident response capability (the NASA *Automated Systems* Incident Response Capability (NASIRC)) which has been in existence at the Goddard Space Flight Center for the past *3 1/2* years.

- NASA has instituted a rigorous risk assessment process that includes determining the relative value, sensitivity, and criticality of information, computing, and communications resources. Various protection, detection, and reaction measures are applied to information, communications, and computing resources based on the criticality of various categories of information (e.g., information about persons, mission-critical information) based on the impact loss or destruction of the information or resources might have.
- NASA participates in a variety of interagency information technology security activities to include National Security Telecommunications and Information Systems Security Committee (NSTISSC), the Information Infrastructure Task Force Security Issues Forum (SIF) *Security Policy Board*, Information Systems Security Organization (ISSO), National Institute of Standards and Technology (NIST) Working Groups, and the Forum of Incident Response and Security Teams (FIRST)
- An effective Agency information technology security program must have top-down senior management support and be appropriately placed in the organizational management structure so that it gets the visibility, attention, and resources it needs to get the job done -- and eliminate unnecessary political conflicts of interest.
- An issue of significant importance to NASA is the capability to conduct business electronically. In order to conduct official business (to include typical commerce activities) over the National Information Infrastructure and the Internet, capabilities must exist for effectively and efficiently applying a digital signature *(authentication)* to documents and enclosing those documents in a *secure* envelope (*encryption*) to prevent unauthorized disclosure or manipulation of *official business, scientific, or engineering data/information.*


Director of Central Intelligence
J. Deutch
National
Intelligence
Council

Organization: National Intelligence Council

Senior Information Assurance Official:

Lawrence K. Gershwin, National Intelligence Officer for Science and Technology
MGen John Landry (Ret.), National Intelligence Officer for General Purpose Forces
Mary McCarthy, National Intelligence Officer for Warning

Information Assurance Points of Contact:

Jeffrey Benjamin, Deputy NIO/S&T

On-Line Resources:

Information Assurance Related Missions and Functions:

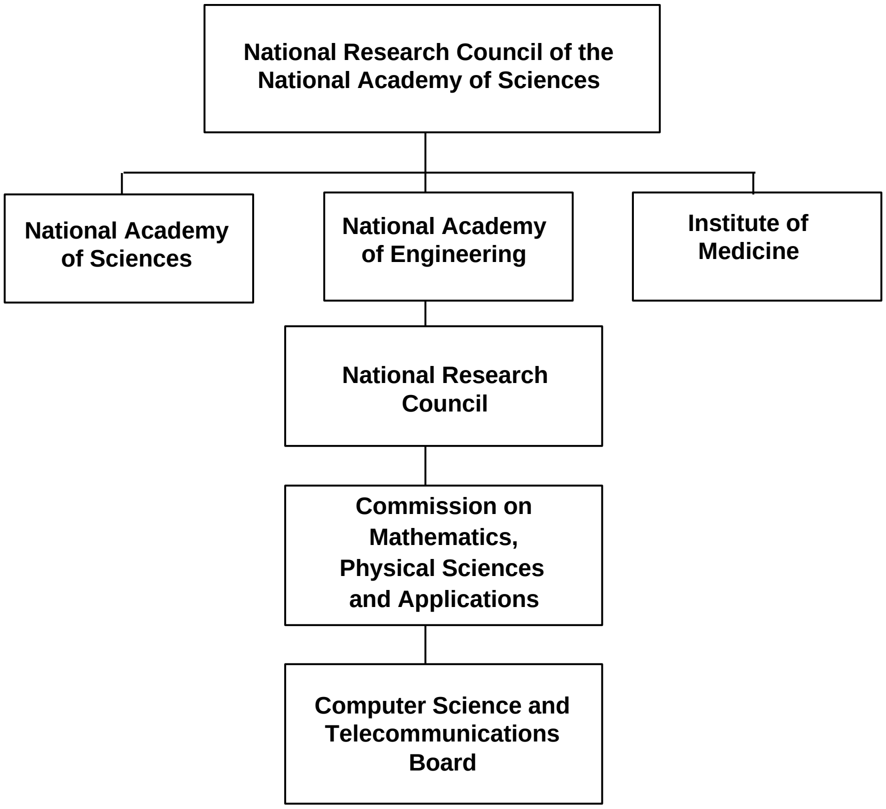
The National Intelligence Council serves as a senior advisory group to the Director of Central Intelligence. National Intelligence Officers (NIOs) support the DCI in his capacity as head of the Intelligence Community by producing interagency reports and analysis, including National Intelligence Estimates.

The NIO for Science and Technology addresses threat issues associated with foreign information warfare plans, programs, and capabilities. Current emphasis is on threats to critical US national-level infrastructures, including the financial sector, electric power distribution, and telecommunications. An Intelligence Community Assessment was completed in 1995, and a more comprehensive NIE on this subject is scheduled for completion by 1 December 1996.

The NIO for General Purpose Forces addresses IW-related threats to US military forces in theater and information-dependent weapon systems.

The NIO for Warning addresses issues associated with indications and warnings for IW. She is sponsoring a DIA-led effort to develop indicators which will help warn of planned or impending IW attacks.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:


National Research Council of the National Academy of Sciences
National Academy of Sciences
National Academy of Engineering
Institute of Medicine
National Research Council
Commission on Mathematics, Physical Sciences and Applications
Computer Science and Telecommunications Board

Organization: National Research Council of the National Academy of Sciences

Senior Information Warfare Official:

Information Warfare Points of Contact:

Marjorie Blumenthal, Director, Computer Science and Telecommunications Board
Herbert Lin, Senior Staff Officer

On-Line Resources:

NRC Homepage: http://www.nas.edu/nrc/

Information Warfare Related Missions and Functions:

The Computer Science and Telecommunications Board (CSTB) is an operating unit within the Commission on Mathematics, Physical Sciences, and Applications of the National Research Council (NRC). The National Research Council is the principal working arm of the National Academy of Sciences, National Academy of Engineering, and the Institute of Medicine--three honorific entities to which distinguished experts in their fields are elected by their peers.

The NRC undertakes work in several major areas of concern: strength of the nation's scientific and technological research and development capabilities; replenishment of scientific and engineering personnel; growth of innovation and productivity; human welfare; education; national security; impact of science and technology on government policy; international scientific and technological relations and competition.

Composed of leaders in the field from industry and academia, the CSTB conducts studies of critical national issues that recommend actions or changes in actions by government, industry, and academic researchers. CSTB also provides a neutral meeting ground for consideration and focusing of complex issues where resolution and action may be premature.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- In 1990, the CSTB formed the System Security Study Committee to address the security and trustworthiness of U.S. computing communication systems. The committee was charged with developing a national research, engineering and policy agenda to help the United States achieve a more trustworthy computing technology base by the end of the century. The committee report, *Computers at Risk: Safe Computing in the Information Age*, contains six sets of recommended actions:

  - Promulgating a comprehensive set of generally accepted systems security principles; referred to as GSSP;

- Taking specific short-term actions that build on ready available capabilities;
- Establishing a comprehensive data repository and appropriate education programs to promote public awareness;
- Clarifying export control criteria and procedures;
- Securing funding for a comprehensive, directed program of research; and
- Establishing a new organization to nurture the development, commercialization, and proper use of trust technology, referred to as the Information Security Foundation, or ISF.

- In 1993, the CSTB formed the Committee to Study National Cryptographic Policy. The committee was charged with conducting a comprehensive study of cryptographic technologies and national cryptographic policy. The study assessed the effect of cryptographic technologies on: national security interests of the United States Government; law enforcement interests of the United States Government; commercial interests of United States industry; and privacy interests of United States Citizens. It also assessed the effect of commercial interests of United States industry of export controls on cryptographic technologies.

The committee recently issued its report, "Cryptography's Role in Security the Information Society." The report contained the following recommendations:

A FRAMEWORK FOR NATIONAL CRYPTOGRAPHY POLICY

The framework for national cryptography policy should provide coherent structure and reduce uncertainty for potential vendors and non-government and government users of cryptography in ways that it does not do today. Recommendations 1, 2, and 3 support this basic framework.

Recommendation 1: No law should bar the manufacture, sale, or use of any form of encryption within the United States.

Recommendation 2: National cryptography policy should be developed by the executive and legislative branches on the basis of open public discussion and governed by the rule of law.

Recommendation 3: National cryptography policy affecting the development and use of commercial cryptography should be more closely aligned with market forces.

The committee recognizes that considerations of public safety and national security make it undesirable to maintain an entirely laissez-faire approach to national cryptography policy. But it believes that government intervention in the market should be carefully tailored to specific circumstances. The committee describes a set of appropriate government interventions in Recommendations 4, 5, and 6.

A national cryptography policy that is aligned with market forces would emphasize the freedom of domestic users to determine cryptographic functionality, protection, and implementations according to their security needs as they see fit. Innovation in technologies such as escrowed encryption would be examined by customers for their business fitness of purpose. Diverse user needs would be accommodated; some users will find it useful to adopt some form of escrowed encryption to protect their access to encrypted data, while others will find that the risks of escrowed encryption (e.g., the dangers of compromising sensitive information through a failure of the escrowing system) are not worth the benefits.

Standards are another dimension of national cryptography policy with a significant impact on commercial cryptography and the market. Cryptographic standards that are inconsistent with prevailing or emerging industry practice are likely to encounter significant market resistance. Thus, to the maximum extent possible, national cryptography policy that is more closely aligned with market forces should encourage adoption by the Federal government and private parties of cryptographic standards that are consistent with prevailing industry practice.

Finally, users in the private sector need confidence that products with cryptographic functionality will indeed perform as advertised. To the maximum degree possible, national cryptography policy should support the use of algorithms, product designs, and product implementations that are open to public scrutiny. Information security mechanisms for widespread use that depend on a secret algorithm or a secret implementation invite a loss of public confidence, because they do not allow open testing of the security, they increase the cost of hardware implementations, and they may prevent the use of software implementations as described below. Technical work in cryptography conducted in the open can expose flaws through peer review and assure the private sector user community about the quality and integrity of the work underlying its cryptographic protection.

EXPORT CONTROLS

Recommendation 4: Export controls on cryptography should be progressively relaxed but not eliminated.

Recommendation 4.1: Products providing confidentiality at a level that meets most general commercial requirements should be easily exportable [2].

Recommendation 4.2: Products providing stronger confidentiality should be exportable on an expedited basis to a list of approved companies if the proposed product user is willing to provide access to decrypted information upon legally authorized request.

Recommendation 4.3: The U.S. government should streamline and increase the transparency of the export licensing process for cryptography.

LAW ENFORCEMENT

Recommendation 5: The U.S. government should take steps to assist law enforcement and national security to adjust to new technical realities of the information age.

Recommendation 5.1: The U.S. government should actively encourage the use of cryptography in nonconfidentiality applications such as user authentication and integrity checks.

Recommendation 5.2: The U.S. government should promote the security of the telecommunications networks more actively. At a minimum, the U.S. government should promote the link encryption of cellular communications and the improvement of security at telephone switches.

Recommendation 5.3: To better understand how escrowed encryption might operate, the U.S. government should explore escrowed encryption for its own uses. To address the critical international dimensions of escrowed communications, the U.S. government should work with other nations on this topic.

Recommendation 5.4: Congress should seriously consider legislation that would impose criminal penalties on the use of encrypted communications in interstate commerce with the intent to commit a federal crime.

Recommendation 5.5: High priority should be given to research, development, and deployment of additional technical capabilities for law enforcement and national security to cope with new technological challenges.

PRIVATE SECTOR

Recommendation 6: The U.S. government should develop a mechanism to promote information security in the private sector.

The CSTB has been asked by DARPA to convene a committee that would examine, discuss, and report on interrelated issues relating to research, development, and commercialization of technologies for trustworthy systems. The committee has not been convened at time of publication.

This page intentionally left blank.

Nuclear Regulatory Commission

Organization: United States Nuclear Regulatory Commission (NRC)

Designated Senior Official for Information Resources Management:

Hugh L. Thompson, Jr., Deputy Executive Director for Nuclear Materials Safety, Safeguards, and Operations Support

Information Assurance Points of Contact:

Gerald F. Cranford, Director, Office of Information Resources Management (IRM)
Patricia G. Norry, Director, Office of Administration (ADM)
George H. Messenger, Director, Financial Management, Computer Security and Administrative Support Staff, Office of Information Resources Management (FCAS/IRM)
Raymond J. Brady, Director, Division of Security, Office of Administration, (ADM/SEC)

On-Line Resources:

NRC Homepage: http://www.nrc.gov

Information Assurance Related Missions and Functions:

The mission of the NRC is to ensure that civilian uses of nuclear materials in the United States--in the operation of nuclear power plants and fuel cycle plants, and in medical, industrial, and research applications--are carried out with adequate protection of public health and safety, the environment, and national security.

The NRC accomplishes its purposes by the licensing and regulatory oversight of nuclear reactor operations and other activities involving the possession and use of nuclear materials and wastes; by the safeguarding of nuclear materials and facilities from theft and/or sabotage; by the issuance of rules and standards; and by inspection and enforcement actions.

The NRC was created as an independent agency by the Energy Reorganization Act of 1974, which abolished the Atomic Energy Commission (AEC) and moved the AEC's regulatory function to NRC. This act, along with the Atomic Energy Act of 1954, as amended, provides the foundation for regulation of the nation's commercial nuclear power industry.

The Deputy Executive Director for Nuclear Materials Safety, Safeguards, and Operations Support executes the Executive Director's responsibilities for Nuclear Material Safety and Safeguards (NMSS) programs, including that portion of regional operations dealing with NMSS issues, oversight of enforcement and investigation functions, centralized administrative support services, and centralized information resources management support services.

The Director, Office of Information Resources Management is responsible for the overall direction and management of centralized information resources of the agency in the areas of computer, telecommunications, and information services, including automated systems development and integration, computer operations, database management, data administration, office automation, local and wide area networks, computer and systems security, the Customer Support Center, user training, document control and management, central files, records management, the library, and related technology and information support services to NRC offices.

The Director, Office of Administration is responsible for providing centralized administrative services in the areas of procurement, property management, facilities support, transportation, rulemaking support, Freedom of Information Act requests, publication services, automated graphics, mail and distribution services, local public document rooms, and security.

The Director, Financial Management Computer Security and Administrative Support Staff, Office of Information Resources Management is responsible for managing IRM's financial/administrative support and NRC's computer security program, including reviewing and approving computer security plans; performing risk analyses; providing computer security awareness training; and providing virus protection, eradication and data recovery services.

The Director, Division of Security, Office of Administration, plans, develops, establishes, and administers policies, standards, regulations, and procedures for the overall NRC security program.

Information Assurance Ongoing and Planned Activities:

- Information Security responsibilities are divided in NRC. The Office of Administration is responsible for personnel, facility and information security, including classified information. The Office of Information Resources Management is responsible for unclassified computer and network security.
- A rigorous Information Security Awareness program has just been completed in the agency. A professional video tape was recently developed to allow both Headquarters and Regional managers to efficiently remind employees of the importance of security on information systems.
- The agency is developing a comprehensive Disaster Recovery Plan for Information Systems in the agency.
- The Director IRM serves as Chairman on the National Communications Systems focus team for the National Information Infrastructure.
- The NRC participates in the National Security Telecommunications & Information Systems Security Committee (NSTISSC) as an observer, the National Institute for Standards and Technology (NIST) Federal Computer Security Program Managers' Forum, and the U.S. Security Policy Forum.
- The NRC uses encryption products and restricted access to provide information protection. The agency has conducted penetration studies to determine the robustness of the network security protective mechanisms.

Securities and Exchange Commission
A. Levitt

Organization: Securities and Exchange Commission

Senior Information Assurance Officials:

Information Assurance Points of Contact:

Mike Bartell, Associate Executive Director, SEC Office of Information Technology

On-Line Resources:

SEC Homepage: http://www.sec.gov/

Information Assurance Related Organizations, Missions and Functions:

The SEC is an independent, nonpartisan, quasijudicial regulatory agency with responsibility for administering the federal securities laws. The purpose of these laws is to protect investors in securities markets that operate fairly and ensure that investors have access to disclosure of all material information concerning publicly traded securities. The Commission also regulates firms engaged in the purchase or sale of, people who provide investment advice, and investment companies.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- In May 1996, SEC began mandating the electronic filing of annual reports, 10Qs, and other documents by public companies.

U.S. Postal Service

Postmaster General

Marvin Runyon

Organization: United States Postal Service

Senior Information Assurance Officials:

Richard D. Weirich, Vice President, Information Systems

Information Assurance Points of Contact:

Tim Patterson, Program Manager, Telecommunications, ITSC

On-Line Resources:

USPS Homepage: http://www.usps.gov

Information Assurance Related Organizations, Missions and Functions:

The United States Postal Service provides mail processing and delivery to individuals and businesses within the United States. It is also the responsibility of the Postal Service to protect the mails from loss or theft and to apprehend those who violate postal laws.

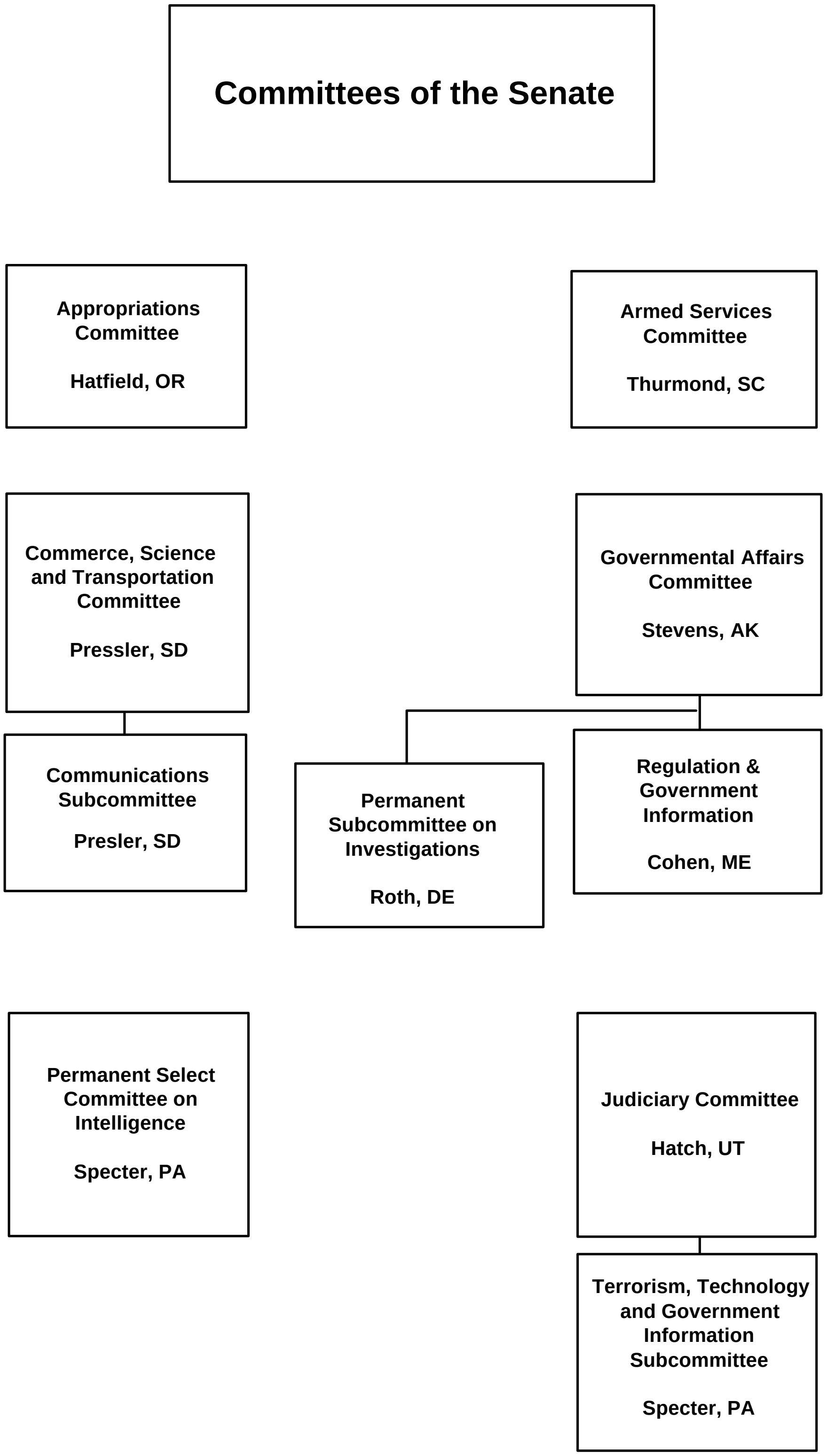
Information Assurance Activities, Issues, Best Practices, Lessons Learned:

This page intentionally left blank.

Legislative and Judicial

Legislative and Judicial

This page intentionally left blank.



Committees of the Senate

Appropriations Committee

Hatfield, OR

Armed Services Committee

Thurmond, SC

Commerce, Science and Transportation Committee

Pressler, SD

Communications Subcommittee

Presler, SD

Governmental Affairs Committee

Stevens, AK

Permanent Subcommittee on Investigations

Roth, DE

Regulation & Government Information

Cohen, ME

Permanent Select Committee on Intelligence

Specter, PA

Judiciary Committee

Hatch, UT

Terrorism, Technology and Government Information Subcommittee

Specter, PA

Organization: Senate

The bulk of the work of preparing and considering legislation in Congress is done in Committees and Subcommittees. The Committee and Subcommittee and Chairpersons listed below may effect activities. IW relevant charters and focus as well as legislative activity are indicated below. Committees are listed in alphabetical order with associated subcommittees and panels.

On-Line Resources:

Senate Homepage: http://www.senate.gov
Thomas legislative information: http://thomas.loc.gov
Roll Call: http://www.rollcall.com

Committee/Subcommittee: Appropriations Committee

Chairman: Sen. Hatfield, Oregon

Information Assurance Related Missions and Functions:

Information Assurance Activities:

- The Committee is faced with funding the Communications Assistance for Law Enforcement Act of 1994. The act mandated but did not appropriate $500 Million over five years to refund to carriers the cost of modifying their equipment.
- Expected to cut DoC operating budget for telecommunications projects such as the NTIA, NII grants, and Advanced Technology Project.

Committee/Subcommittee: Armed Services Committee

Chairman: Sen. Thurmond, South Carolina

Information Assurance Related Missions and Functions:

Defense budget authorization.

Information Assurance Activities:

Committee/Subcommittee: Committee on Commerce, Science and Transportation

Chairman: Sen. Pressler, South Dakota

Information Assurance Related Missions and Functions:

Information Assurance Activities:

Committee/Subcommittee: Commerce Subcommittee on Communications

Chairman: Sen. Larry Pressler, South Dakota

Information Assurance Related Missions and Functions:

Information Assurance Activities:

Committee/Subcommittee: Governmental Affairs Committee

Chairman: Sen. Stevens, Alaska

Information Assurance Related Missions and Functions:

Privacy Act, regulatory issues, government performance and results

Information Assurance Activities:

Committee/Subcommittee: Governmental Affairs Subcommittee on Regulation and Government Information

Chairman: Sen. Cohen, Maine

Information Assurance Related Missions and Functions:

Information Assurance Activities:

- Sen. Cohen sees information technology as the key to improving Federal government management.

Committee/Subcommittee: Governmental Affairs Permanent Subcommittee on Investigations

Chairman: Roth, DE

Information Assurance Related Missions and Functions:

Information Assurance Activities:

- “Security in Cyberspace” Hearings, May-July 1996

Committee/Subcommittee: Permanent Select Committee on Intelligence

Chairman: Sen. Specter, Pennsylvania

Information Assurance Related Missions and Functions:

Intelligence oversight

Information Assurance Activities:

Committee/Subcommittee: Judiciary Committee

Chairman: Sen. Hatch, Utah

Information Assurance Related Missions and Functions:

Information Assurance Activities:

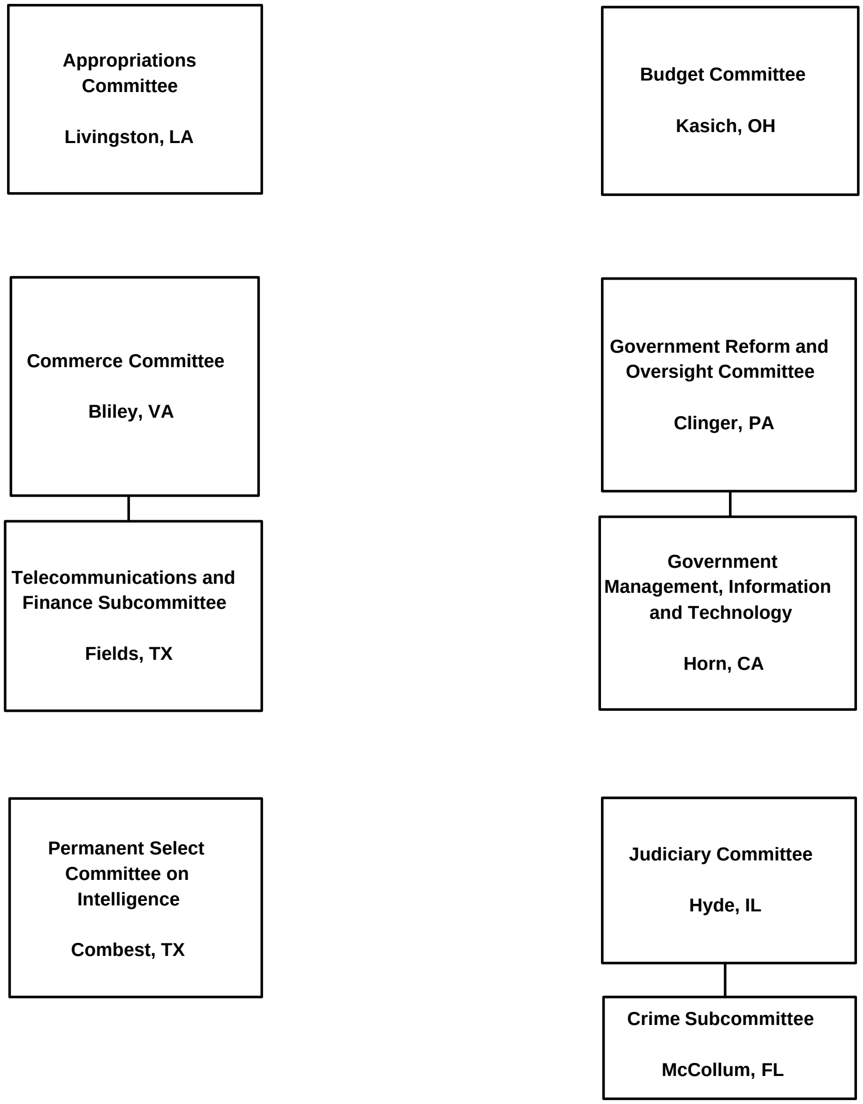
Committee/Subcommittee: Judiciary Subcommittee on Terrorism, Technology and Government Information

Chairman: Sen. Specter, Pennsylvania

Information Assurance Related Missions and Functions:

Information Assurance Activities:

Committees of the House of Representatives



Appropriations Committee

Livingston, LA

Budget Committee

Kasich, OH

Commerce Committee

Bliley, VA

Telecommunications and Finance Subcommittee

Fields, TX

Government Reform and Oversight Committee

Clinger, PA

Government Management, Information and Technology

Horn, CA

Permanent Select Committee on Intelligence

Combest, TX

Judiciary Committee

Hyde, IL

Crime Subcommittee

McCollum, FL

Organization: House of Representatives

The bulk of the work of preparing and considering legislation in Congress is done in Committees and Subcommittees. The Committee and Subcommittee and Chairpersons listed below may affect IW activities. IW relevant charters and focus as well as legislative activity are indicated below. Committees are listed in alphabetical order with associated subcommittees and panels.

On-Line Resources:

House Homepage: http://www.house.gov
Thomas legislative information: http://thomas.loc.gov
Roll Call: http://www.rollcall.com

Committee/Subcommittee: Appropriations Committee

Chairman: Rep. Livingston, Louisiana

Information Assurance Related Missions and Functions:

Budget

Information Assurance Activities:

Committee/Subcommittee: Budget Committee

Chairman: Rep. Kasich, Ohio

Information Assurance Related Missions and Functions:

Budget

Information Assurance Activities:

Committee/Subcommittee: Commerce Committee

Chairman: Rep. Bliley, Virginia

Information Assurance Related Missions and Functions:

Federal Communications Commission

Information Assurance Activities:

Committee/Subcommittee: Commerce Subcommittee on Telecommunications and Finance

Chairman: Rep. Fields, Texas

Information Assurance Related Missions and Functions:

Privacy, telecommunications, finance

Information Assurance Activities:

- Prepared House Telecommunications Reform Bill

Committee/Subcommittee: Government Reform and Oversight Committee (formerly Government Operations Committee)

Chairman: Rep. Clinger, Pennsylvania

Information Assurance Related Missions and Functions:

Civil Service, Postal Service, Washington DC, oversight

Information Assurance Activities:

- Rep. Clinger plans to take the lead role in communicating federal agency information technology needs to the House.
- Rep. Clinger cosponsored the Paperwork Reduction Act.

Committee/Subcommittee: Government Reform and Oversight Subcommittee on Government Management, Information, and Technology (New subcommittee)

Chairman: Rep. Horn, California

Information Assurance Related Missions and Functions:

Privacy Act, NII, paperwork reduction, Federal Agencies

Information Assurance Activities:

Committee/Subcommittee: Permanent Select Committee on Intelligence

Chairman: Rep. Combest, Texas

Information Assurance Related Missions and Functions:

Intelligence oversight

Information Assurance Activities:

Committee/Subcommittee: Judiciary Committee

Chairman: Rep. Hyde, Illinois

Information Assurance Related Missions and Functions:

Information Assurance Activities:

Committee/Subcommittee: Judiciary Subcommittee on Crime

Chairman: Rep. McCollum, Florida

Information Assurance Related Missions and Functions:

FBI, criminal justice

Information Assurance Activities:

Committee/Subcommittee: Committee on National Security (Formerly House Armed Services Committee)

Chairman: Rep. Spence, South Carolina

Information Assurance Related Missions and Functions:

Defense Budget “authorizers”

Information Assurance Activities:

Committee/Subcommittee: Science Committee

Chairman: Rep. Walker, Pennsylvania

Information Assurance Related Missions and Functions:

Information Assurance Activities:

- Rep. Walker is concerned that U.S. standards process is limiting international trade.

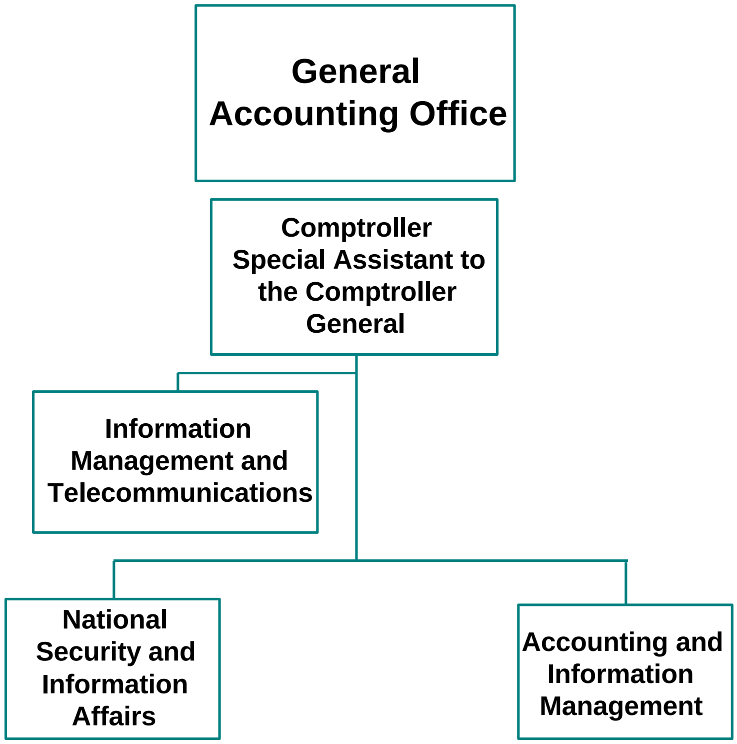
Committee/Subcommittee: Science Subcommittee on Technology

Chairman: Rep Morella, Maryland

Information Assurance Related Missions and Functions:

Information Assurance Activities:

This page intentionally left blank.



General Accounting Office

Comptroller Special Assistant to the Comptroller General

Information Management and Telecommunications

National Security and Information Affairs

Accounting and Information Management

Organization: General Accounting Office (GAO)

Senior Information Assurance Officials:

F. Kevin Boland, Assistant Comptroller General, Office of Information Management and Communications
Jack Brock, Director of Information Resources Management
Butch Hinton, Assistant Comptroller General, National Security and International Affairs Division

Information Assurance Points of Contact:

On-Line Resources:

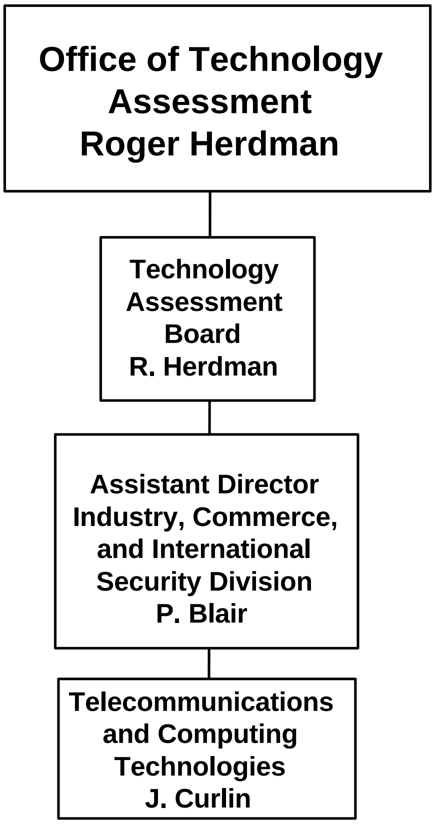
GAO Homepage: http://www.gao.gov

Information Assurance Related Missions and Functions:

The General Accounting Office (GAO) is the audit and investigative arm of the Congress. Its primary function is to respond to requests from Congress for audits and evaluations of government programs and agencies. The GAO also works closely with the Office of Management and Budget and the Secretary of the Treasury to standardize Federal government information systems. The GAO also prescribes accounting standards for the Executive Branch.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- GAO continues to find examples of poor information security during audits and investigations.
- Reports issued in 1989, 1991, and 1993 highlight problems with virus' on the Internet, privacy invasions by federal employees, and penetrations of DoD computer systems.
- Internally, GAO has installed Internet connections with firewalls.
- In May 1996, the GAO released a report to Congress entitled *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* [GAO 1]. On May 22, 1996, GAO testified on their investigation on the first day of hearings on computer security conducted by the Senate Permanent Subcommittee on Investigations, Committee on Governmental Affairs.



Office of Technology Assessment
Roger Herdman

Technology Assessment Board
R. Herdman

Assistant Director
Industry, Commerce, and International Security Division
P. Blair

Telecommunications and Computing Technologies
J. Curlin

Organization: Office of Technology Assessment (OTA)

The OTA was unfunded by Congress in FY 96.

Senior Information Assurance Official:

James Curlin, Program Director, Telecommunications and Computing Technologies

Information Assurance Points of Contact:

On-Line Resources:

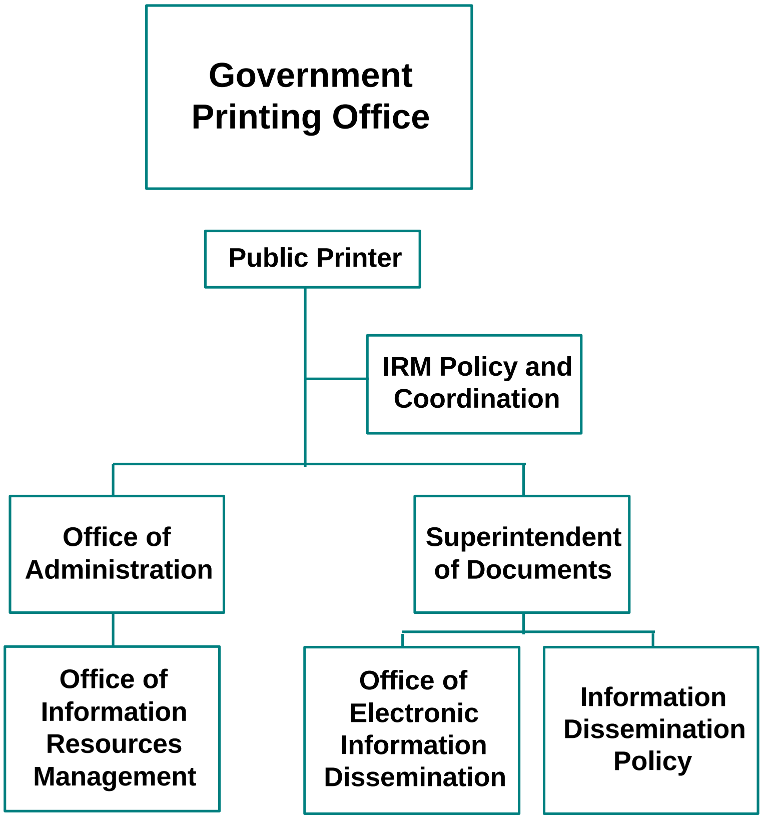
OTA Homepage: http://www.ota.gov

Information Assurance Related Missions and Functions:

The Office of Technology Assessment (OTA) "reports to Congress on the scientific and technical impact of government policies and proposed legislative initiatives." [Office of the Federal Register, 1994] It receives guidance and assignments from a Congressional Board and advice from a Technology Assessment Advisory Council. Its assessments are comprehensive; often taking one to two years to complete, and authoritative as each OTA assessment team is advised by a panel of experts.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- OTA reports are comprehensive, authoritative, and readable and are available from the U.S. Government Printing Office.
- In June 1995, OTA published an issue update [OTA 2] of their 1994 report entitled *Information Security and Privacy in Network Environments [OTA 1].* These reports provide useful summaries of the privacy and security background and issues associated with computer networks.


Government Printing Office
Public Printer
IRM Policy and Coordination
Office of Administration
Superintendent of Documents
Office of Information Resources Management
Office of Electronic Information Dissemination
Information Dissemination Policy

Organization: Government Printing Office

Senior Information Assurance Officials:

Patricia R. Gardner, Director of Information Resources Management
Judith Russell, Director of Electronic Information Dissemination Services

Information Assurance Points of Contact:

On-Line Resources:

GPO Homepage: http://www.access.gpo.gov

Information Assurance Related Missions and Functions:

The Government Printing Office (GPO) prints, binds, and distributes documents for the Federal government. It has special statutory authority to make documents available electronically to the public free of charge. It is better known for selling government publications through mail order and GPO bookstores at reasonable prices. It also produces and provides documents on CD-ROM, operates File Transfer Protocol and World Wide Web sites and makes information available through the Federal Bulletin Board.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

Commission on Protecting and Reducing Government Secrecy

Organization: Commission on Protecting and Reducing Government Secrecy

Senior Information Assurance Official:

Jacques Rondeau, Deputy Staff Director

Information Assurance Point of Contact:

Michael J. White, Senior Professional Staff

On-Line Resources:

Information Assurance Related Missions and Functions:

In examining how to arrive at recommended reforms, the Commission will be guided by the broad interest in careful analysis of the costs -- both qualitative and quantitative --of classification, declassification, and personnel security measures. It also will consider the extent to which there has developed a bureaucratic "culture" generally resistant to change in recent years based on the efforts of senior management at certain agencies as well as outside observers such as the Joint Security Commission. Such an examination will be coupled with a consideration of how best to promote greater "accountability" on the part of those charged with designing and implementing security programs.

Technological innovations present both opportunities and challenges to those responsible for protecting and reducing government secrecy--though many of these consequences only are beginning to be understood within the Federal government and elsewhere.

Information Assurance Activities, Issues, Best Practices, Lesson Learned:

The Impact of Technology on Protecting and Reducing Secrecy

- How is the Government organized to address the effects of technological developments on security policies and procedures?
- How can technology improve public access to information?
- How can technology improve security clearance procedures and the transfer of clearances between agencies?
- How can technology contribute to better protection of classified and sensitive but unclassified information?
- How can technology be used to standardize information systems security?
- How does technology affect the management of security decisionmaking and the formulation of security policies throughout the Government?

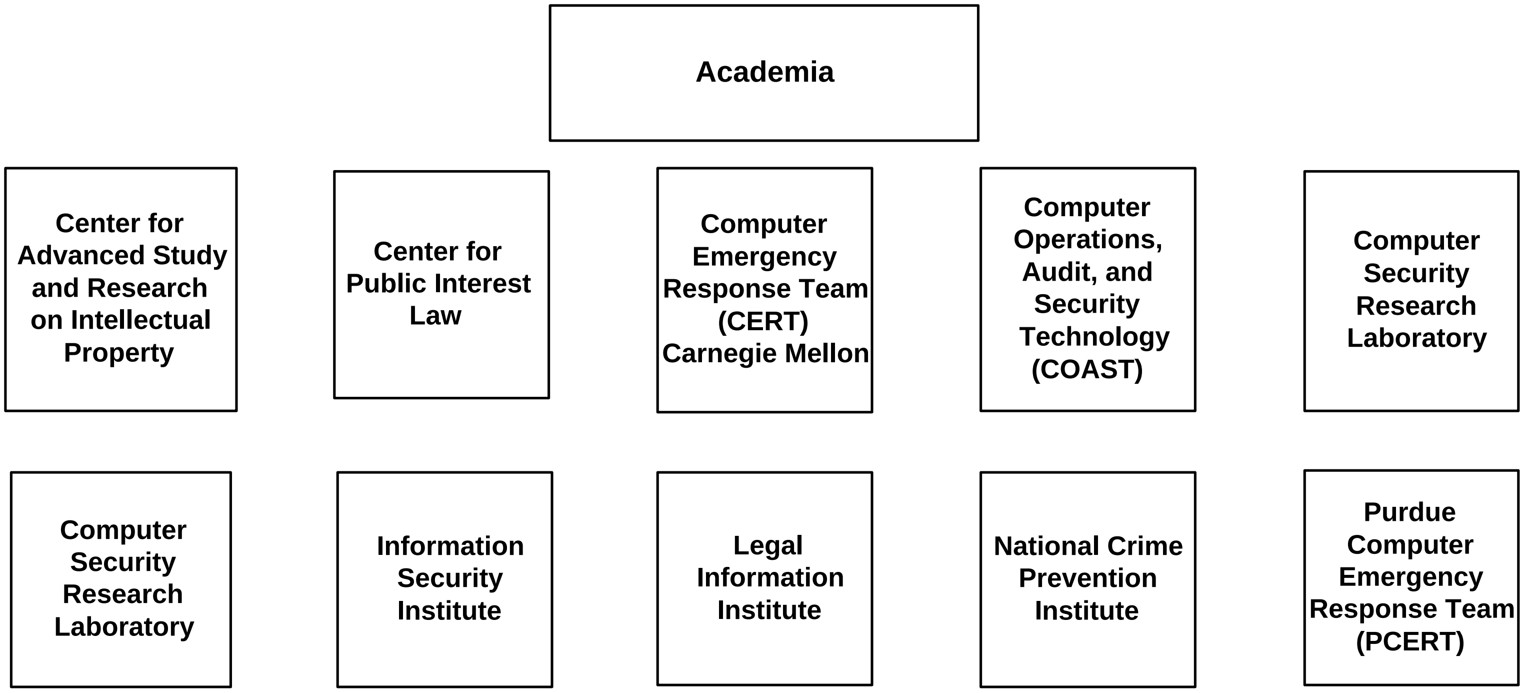
This page intentionally left blank.

International, National, State and Local

[redacted]

International, National, State & Local

This page intentionally left blank.



Academia

Center for Advanced Study and Research on Intellectual Property

Center for Public Interest Law

Computer Emergency Response Team (CERT) Carnegie Mellon

Computer Operations, Audit, and Security Technology (COAST)

Computer Security Research Laboratory

Computer Security Research Laboratory

Information Security Institute

Legal Information Institute

National Crime Prevention Institute

Purdue Computer Emergency Response Team (PCERT)

PUBLIC ORGANIZATIONS

ACADEMIA

Center for Advanced Study and Research on Intellectual Property (CASRIP)

University of Washington School of Law, Seattle, WA

URL: http://www.law.washington.edu:80/~casrip/

CASRIP is an independent research and policy development institute focusing on problems in patent and other property ownership rights in the products of high technology. It aims to improve discussion and exchange of views between professionals of various countries, particularly those countries that have major intellectual property systems.

Center for Public Interest Law

University of San Diego School of Law, 5998 Alcala Park, San Diego, CA 92110-2492

URL: http://pwa.acusd.edu/~prc/index.html

This center serves as an academic center of research, learning, and advocacy in administrative law. This center also administers the Privacy Rights Clearinghouse. This Clearinghouse is funded by the Telecommunications Education Trust, a program of the California Public Utilities Commission, and its purpose is to raise consumers' awareness of how technology affects personal privacy.

Computer Emergency Response Team (CERT)

Coordination Center, Software Engineering Institute, Carnegie Mellon University,
Pittsburgh, PA 15213-3890

412/268-7090

Lucy Piccolino, Information Coordinator, 412/268-7700

URL: http://www.sei.cmu.edu/SEI/programs/cert/CERT.info.html

The CERT charter is to work with the Internet community to facilitate its response to computer security events involving Internet hosts, to take proactive steps to raise the community's awareness of computer security issues, and to conduct research targeted at improving the security of existing systems. CERT products and services include a 24-hour technical assistance for responding to computer security incidents, products vulnerability assistance, technical documents, and seminars.

Computer Operations, Audit, and Security Technology (COAST)

Department of Computer Sciences, Purdue University, West Lafayette, IN 47907-1398

URL: http://www.cs.purdue.edu/coast/coast.html

This is a multiple project, multiple investigator effort in computer security research. COAST functions with close ties to researchers and engineers in major companies and government agencies. The focus of their research is on real-world needs and limitations.

Computer Security Research Laboratory

Computer Sciences Department, University of California, 2245 Engineering Unit II, Davis, CA

916/752-2149

URL: http://seclab.cs.ucdavis.edu/

Research in the Computer Security Research Laboratory is concerned with the development of new techniques for the design of secure systems and for demonstrating such systems to be secure. Current research activities include: (1) developing techniques for understanding malicious code and for detecting and preventing the occurrence of such code in programs, and (2) developing techniques for network intrusion detection. The intent is to flag network intruders and abusers with a low probability of false alarms. The basic philosophy is to employ rule-based approaches to detect policy violations or attempts at exploiting system vulnerabilities. A current project is developing an intrusion detection system that could be used on the INTERNET.

Information Security Institute

George Mason University, Center for Professional Development, 4400 University Drive, Fairfax, VA 22030-4440

URL: http://www.isse.gmu.edu/~gmuisi/

Legal Information Institute

Cornell Law School, Myron Taylor Hall, Ithaca, NY 14853

URL: http://www.law.cornell.edu/index.html

This institute aims to explore new ways of distributing legal documents and commentary. One primary aim is the dissemination of legal information via the Internet.

National Crime Prevention Institute

University of Louisville, Belknap Campus, Brigman Hall, Louisville, KY 40292

502/852-6987

Wilbur Rykert, Director

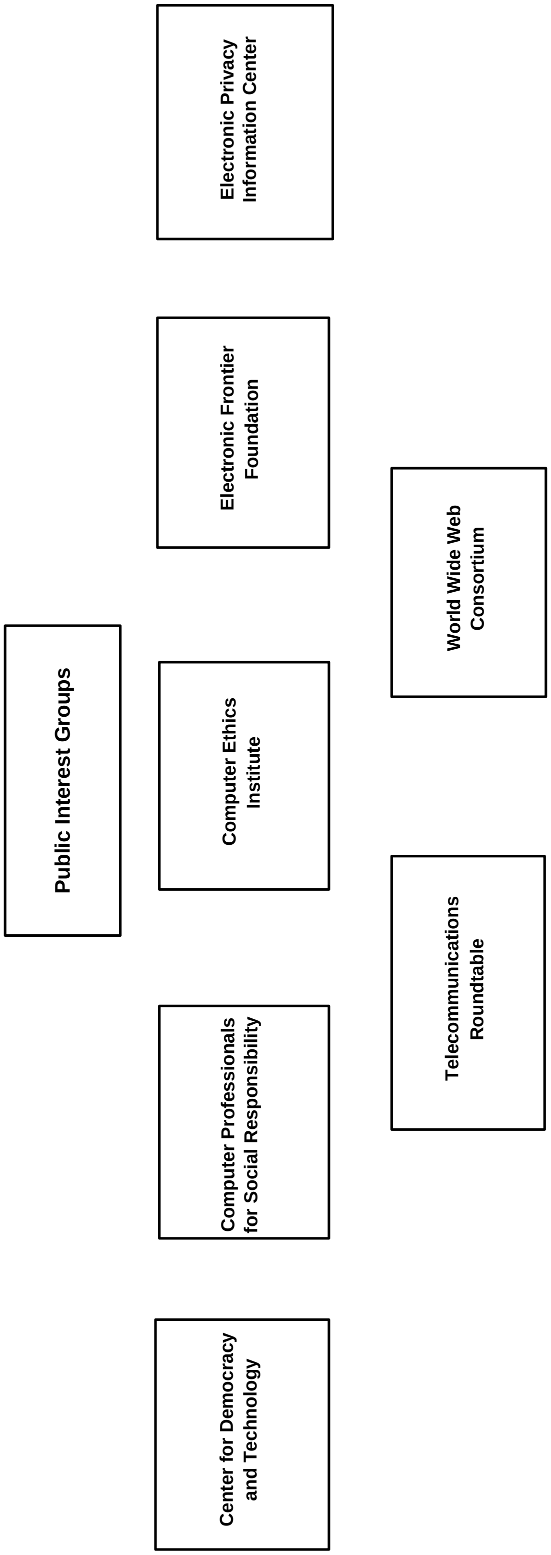
This Institute engages in research pertaining to physical and electronic security and review of loss reduction techniques. The institute trains police officers, criminal justice planners, security personnel in the private sector and community representatives in crime prevention

Purdue Computer Emergency Response Team (PCERT)

Purdue University, Lafayette, Indiana

URL: http://www.cs.purdue.edu/pcert/pcert.html

PCERT is a team of faculty and staff at Purdue University who work together to improve computer security, advise on policies regarding computer use and misuse, and who coordinate responses to computer security incidents on campus. The PCERT is the first university response team admitted to membership in the FIRST.


Public Interest Groups
Center for Democracy and Technology
Computer Professionals for Social Responsibility
Computer Ethics Institute
Electronic Frontier Foundation
Electronic Privacy Information Center
Telecommunications Roundtable
World Wide Web Consortium

PUBLIC ORGANIZATIONS

PUBLIC INTEREST GROUPS

Center for Democracy and Technology

Washington, DC

Jerry Berman

URL: http://www.cdt.org/

This is a non-profit public interest organization; its mission is to develop and advocate public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies. The Center achieves its goals through policy development, public education, and coalition building.

Computer Professionals for Social Responsibility (CPSR)

P.O. Box 717, Palo Alto, CA 94302

415/322-3778

URL: http://snyside.sunnyside.com/home/

This is a non-profit, public interest organization concerned with the effects of computers on society. The mission of CPSR is to provide the public and policymakers with realistic assessments of the power, promise, and problems of information technology.

Electronic Frontier Foundation (EFF)

1550 Bryant Street, Suite 725
San Francisco CA 94117 USA

415 436 9333 (voice)
415 436 9993 (fax)

URL: http://www.eff.org

The EFF is a non-profit, civil liberties, public interest organization founded in July 1990 to ensure that the principles embodied in the Constitution and the Bill of Rights are protected as new communications technologies emerge. The work of this organization focuses on protection of privacy and access to on-line resources and information.

Electronic Privacy Information Center (EPIC)

666 Pennsylvania Avenue, SE, Suite 301, Washington, DC 20003

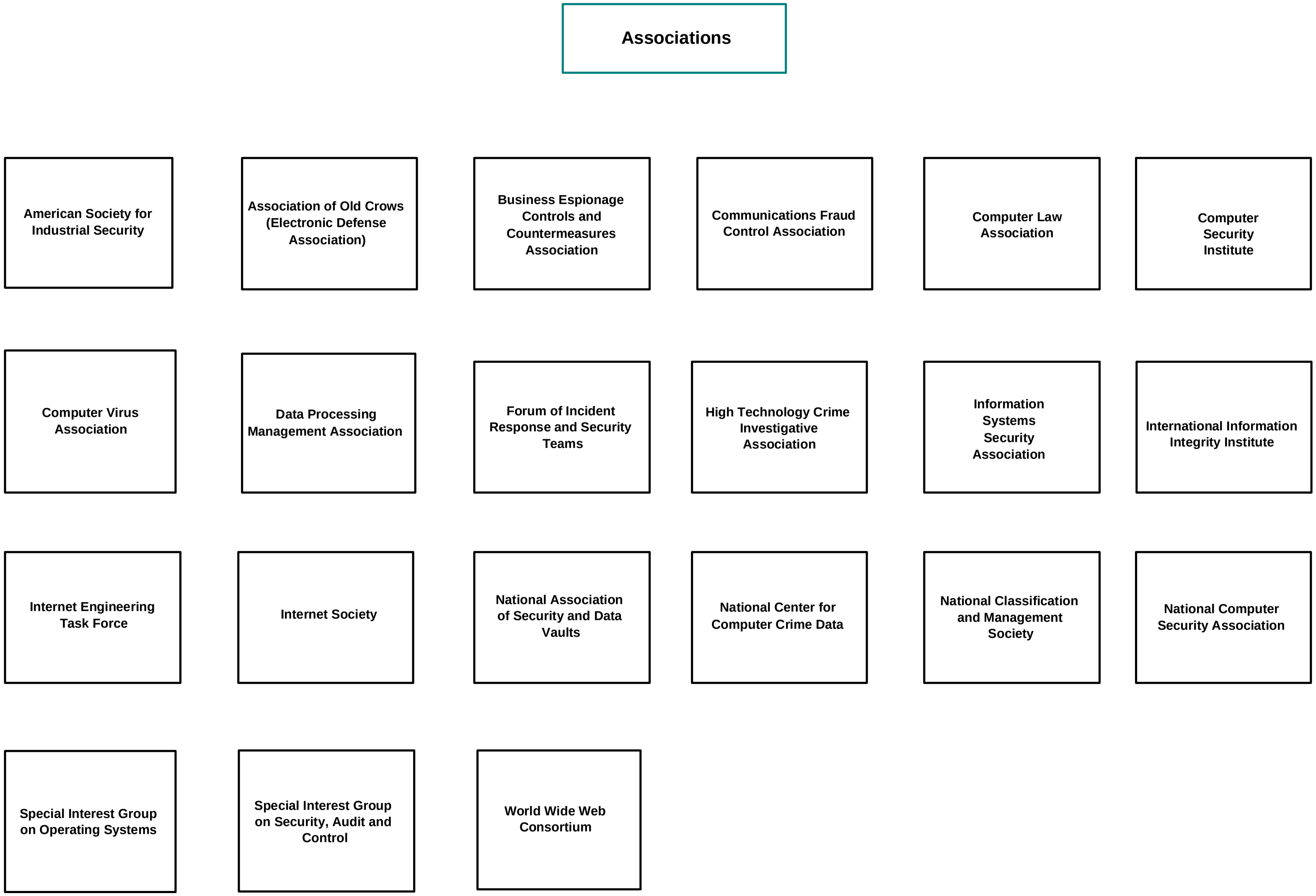
202/544-9240

Marc Rotenburg, Director
David Sobel, Legal Counsel

URL: http://washofc.epic.org/

This public policy group advocates for electronic privacy. It is a public interest research center, established in 1994 to focus public attention on emerging privacy issues relating to the National Information Infrastructure (NII). It supports efforts to preserve the right of privacy in the electronic age, to give individuals greater control over personal information, and to encourage the development of new technologies that protect privacy rights. It sponsors educational and research programs, a speakers' bureau, compiles statistics, and conducts litigation. It is currently suing the NSC for details on the proposal for NSC to assume oversight of federal information security (see U.S. Security Policy Board).

This page intentionally left blank.



Associations

American Society for Industrial Security

Association of Old Crows (Electronic Defense Association)

Business Espionage Controls and Countermeasures Association

Communications Fraud Control Association

Computer Law Association

Computer Security Institute

Computer Virus Association

Data Processing Management Association

Forum of Incident Response and Security Teams

High Technology Crime Investigative Association

Information Systems Security Association

International Information Integrity Institute

Internet Engineering Task Force

Internet Society

National Association of Security and Data Vaults

National Center for Computer Crime Data

National Classification and Management Society

National Computer Security Association

Special Interest Group on Operating Systems

Special Interest Group on Security, Audit and Control

World Wide Web Consortium

PRIVATE ORGANIZATIONS

ASSOCIATIONS

American Society for Industrial Security

1655 North Fort Myer Drive, Suite 1200, Arlington, VA 22209

703/522-5800

Michael Stack, Executive Director; F. Joseph Ricci, Director of Marketing

URL: http://all.net/journal/asis/top.html

This organization acts as a conduit for security professionals; it provides programs and resources at all local, national, and international levels which enable members to update and exchange information and expertise. The role of ASIS Standing Committees and Councils is to keep members informed of the latest developments in security practice and technology and to further integrate specialized knowledge and skills. The ASIS has 27 standing committees, 6 subcommittees, and 3 councils.

- Computer Security Committee: John Spain, Chairman. 404/614-4141.
- Disaster Management Committee: Robert Lee, Chairman. 818/775-4099.
- Government Security Committee: Cynthia Conlon, Chairman. 310/393-0411 X7201.
- Telecommunications Committee: Robert Postovit, Chairman. 206/345-7351.
- Terrorist Activities Committee: Robert Disney, Chairman. 718/481-6400.
- White Collar Crime Committee: Frederick Verinder, Chairman. 202/324-4805.

Association of Old Crows (Formerly the Electronic Defense Association)

1000 N. Payne St., Alexandria, VA 22314

703/549-1600

Gus Slayton, Director

URL: http://www.jedefense.com/jed.html

This is a professional association of scientists, engineers, managers, operators, educators, military personnel and others engaged in the science of electronic warfare and related areas. Approximately 23000 members in 92 regional groups.

Business Espionage Controls and Countermeasures Association

P.O. Box 55582, Seattle, WA 98155

206/364-4672

William Johnson, Executive Director

This association has management consultants, law enforcement officials, and information specialists involved in business espionage controls and countermeasures. Promotes business awareness of the growing concern of espionage in the business community. It publishes "The Business Espionage Report" monthly.

Communications Fraud Control Association

1990 M Street, NW, Suite 508, Washington, DC 20036

202/296-3225

Frances Feld, Executive Director

The thrust of the Association is to find effective ways to combat the growing problem of communications fraud. The Association has the following missions:

- Serves as a clearinghouse for telecommunications fraud information
- Develops training programs on the latest anti-fraud technologies
- Supports legislative protection
- Improve investigative standards and techniques.

Membership includes representatives from MCI, AT&T, SBS, ITT, Network One, many of the Bell Operating Companies and smaller resellers of telecommunications services.

Membership categories include PBX owners, Corporate end-users (Dupont, J.C. Penny, hospitals and universities), International PTTs, Operator Service Providers, Independent Public Payphone Providers, Secret Service and FBI agents, local and Canadian provincial authorities, prosecutors and telecommunication consultants.

Computer Law Association, Inc.

3028 Javier Road, Suite 402, Fairfax, VA 22031
(703) 560-7747 (v) (703) 207-7028 (f)

Founded in 1971, the Computer Law Association has over 1,600 members in thirty-eight countries. The Computer Law Association's non-profit purpose is to inform and educate lawyers about the unique legal issues arising from the evolution, production, marketing, acquisition and use of computer-communications technology. The CLA has sponsored programs and seminars covering a wide-range of topics involving computer law. Such topics include financing, taxation, commercial, contracting, tort liability, and intellectual property rights.

Computer Security Institute

600 Harrison Street, San Francisco, CA 94107

415/905-2370

Patrice Rapalus, Director

URL: http://www.gocsi.com/HomePage.html

Provides computer and information security professionals with information resources and support through membership, training, conferences and networking opportunities. Membership includes many major American Corporations: Aetna Life & Casualty, Allstate Insurance, AT&T, Blue Cross, Boeing Information Services, Chase Manhattan Bank, Coca-Cola Company, Dean Wittier, Dow Chemical, Dupont, Eastman Kodak, Exxon, etc.

Computer Virus Association

408/727-4559

John McAfee, Chairman

This association offers assistance to companies involved in identifying and eradicating computer viruses. It conducts research programs and compiles statistics. Approximately 60 members.

Data Processing Management Association

505 Busse Highway, Park Ridge, IL 60068

708/825-8124

Suzanne Lattimore

URL: http://negaduck.cc.vt.edu/DPMA/

Membership is made up of managerial personnel, staff, educators, and individuals interested in management of information resources. It maintains a Legislative Communications Network, professional education programs, and sponsors student organizations around the country. Membership numbers 24000 in 12 regional groups and 275 local groups.

Forum of Incident Response and Security Teams (FIRST)

National Institute of Standards and Technology, A-216 Technology. Gaithersburg, MD 20899

301/975-3359

URL: http://first.org/first/

FIRST is an international consortium which brings together a variety of computer security incident response teams from government, commercial, and academic organizations. It aims to foster cooperation and coordination in incident prevention, to provide members with technical information, tools, methods, assistance, and guidance, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large.

High Technology Crime Investigative Association (HTCIA)

P.O. Box 162034, Sacramento, CA 95816

916/441-1333

The HTCIA encourages, promotes, aids and effects the voluntary interchange of data, information, experience, ideas, and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies among its membership.

Information Systems Security Association, Inc.

800 N. Lingbergh, G2EE, St. Louis, MO 63167

314/694-7661

Ms. Genevieve M. Burns (of Monsanto Corp.), President

URL: http://www.uhsa.uh.edu/issa/

This is an international organization providing educational forums, publications and peer interaction opportunities. The primary goal of ISSA is to promote management practices that will ensure availability, integrity and confidentiality of organizational resources.

Membership: greater than 2,000. Includes major U.S. and international corporations, leading consulting firms, government agencies, and educational institutions. Has more than 35 chapters in major American cities.

International Information Integrity Institute (I4)

333 Ravenswood Avenue, Menlo Park, CA 94025

415/859-4771

Dr. Bruce Baker, Program Manager, SRI International

Assists major enterprises and government agencies in protecting their information assets; I4 is dedicated to advancing information security and enterprise protection by encouraging prudent management responsibilities that lead to a standard of due care.

Internet Engineering Task Force (IETF)

c/o Corporation for National Research Initiatives, 1895 Preston White Drive, Suite 100, Reston, VA

703/620-8990

G. Malkin, IETF Secretariat

URL: http://www.ietf.cnri.reston.va.us/

The IETF is the protocol engineering and development arm of the Internet. It is a large, self-organized, open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual but there isn't any membership in the IETF. Actual technical work of the IETF is done in its working groups (routing, network management, and security). The mission of the IETF includes: (1) identifying and proposing solutions to pressing operational and technical problems in the Internet, (2) specifying the development or usage of protocols and the near-term architecture to solve such technical problems for the Internet, (3) making recommendations to the Internet Engineering Steering Group (IESG), (4) facilitating technology transfer from the Internet Research Task Force (IRTF) to the wider Internet community, and (5) providing a forum for the exchange of information within the Internet community.

Internet Society

12020 Sunrise Valley Drive, Suite 270, Reston, VA 22091

703/648-9888

Vinton G. Serf, President

URL: http://info.isoc.org/home.html

A nongovernmental, international organization for global cooperation and coordination for the Internet and its technologies and applications. Principal purpose is to maintain and extend the development and availability of the Internet and its associated technologies and applications.

National Association of Security and Data Vaults

716 E. Washington Str., Syracuse, NY 13210

315/475-7743

Ellie Seitz, President

This association has individuals and firms in the private security vault and data storage business. Its accredited members are vault businesses that have met standards set forth by the association. It promotes establishment of non-bank, high-security centers for data storage operations. The association has about 80 members.

National Center for Computer Crime Data

1222 17th Ave., Suite B, Santa Cruz, CA 95062

408/475-4457

Jay J. Bloombecker, Director

This organization is made up of individuals and organizations in the security, law enforcement, legal, business, accounting, and computing professions. It facilitates the prevention, investigation, and prosecution of computer crime by disseminating documents and other data to those in need of such information.

National Classification and Management Society

6118 Roseland Drive, Rockville, MD 20852

301/231-9191

Eugene J. Suto, Executive Secretary

This society manages, supervises, and performs in a security classification management capacity in industry, government, the military services, and educational institutions. The society seeks to establish systems and techniques for identifying information or materials requiring protection in the national interest; it also helps establish procedures and practices for management of classified materials. The society has about 2300 members in 29 local groups.

National Computer Security Association

10 South Courthouse Avenue, Carlisle, PA 17013

717/258-1816

Robert Bales, Executive Officer. Paul Gates, Membership Director

URL: http://www.ncsa.com/

This is a membership organization which provides educational materials, training, testing, and consulting services to improve computer and information security, reliability and ethics.

Special Interest Group on Operating Systems

University of Washington, Department of Computer Sciences, FR-35, Seattle, WA 98195

208/543-9204

Henry Levy, Chairman

URL: http://www.acm.org/sigops/

A special interest group of the Association for Computing Machinery. The group is made up of individuals interested in reliability, integrity and security of data, computer operating systems, communications among computing processes, and much more. Approximately 8100 members.

Special Interest Group on Security, Audit and Control

Association for Computing Machinery, 1515 Broadway, New York, NY 10036

212/869-7440

Daniel Faigin, Chairman

URL: http://www.acm.org/sig_hp/sigsac.html

A special interest group of the Association for Computing Machinery. The groups is made up of information processing security personnel, auditors, accountants and computer technicians. Its purpose is to maintain high levels of skill and awareness regarding technology and practice in the fields of computer security, audit, and control. Approximately 1300 members.

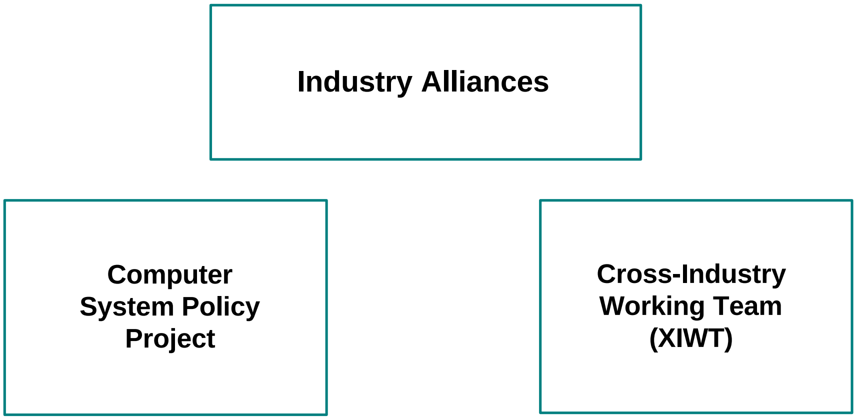
World Wide Web Consortium

Massachusetts Institute of Technology
Laboratory for Computer Science
545 Technology Square
Cambridge, MA 02139

617-253-2613

URL: http://www.w3.org/pub/WWW/

The W3 Consortium exists to develop common standards for the evolution of the World Wide Web. It is an industry consortium run by the Laboratory for Computer Science at the Massachusetts Institute of Technology.



Industry Alliances

Computer System Policy Project

Cross-Industry Working Team (XIWT)

PRIVATE ORGANIZATIONS

INDUSTRY ALLIANCES

Cross-Industry Working Team (XIWT)

c/o Corporation for National Research Initiatives, 1895 Preston White Drive, Suite 100,
Reston, VA, 22091

703/620-8990

Charles N. Brownstein, Executive Director

URL: http://merlin.cnri.reston.va.us:3000/XIWT/

XIWT is a multi-industry coalition committed to defining the architecture and key technical requirements for a powerful and sustainable national information infrastructure (NII). It aims to foster understanding, development and application of technologies that cross industry boundaries, to facilitate the conversion of the NII vision into real-world implementations, and to facilitate a dialogue among representatives of stakeholders in the private and public sectors.

Computer Systems Policy Project

c/o Pam Fandel, Computer System Policy Project, 1735 New York Avenue, NW,
Suite 500, Washington, DC 20006

202/662-8403

URL: http://www.podesta.com/cspp/index.html

The Computer Systems Policy Project (CSPP) is an affiliation of chief executive officers of American computer companies that develop, build, and market information processing systems and software. CSPP's members include the chief executives of Apple, AT&T, Compaq, Control Data Systems, Cray Research, Data General, Digital Equipment, Hewlett-Packard, IBM, Silicon Graphics, Sun Microsystems, Tandem, and Unisys. Upon forming CSPP in 1989, the CEOs made a commitment to work together to develop and personally advocate public policy positions on trade and technology issues that affect their industry, all high-technology industries, and hence, the nation. To date, CSPP has issued numerous reports which outlines the CEO's positions on a variety of issues.

This page intentionally left blank.

Points of Contact

Points of Contact

POINTS OF CONTACT

Three points of contact lists have been provided for the reader’s convenience. The first two offer the same information in slightly different formats. The third provides contact information for computer emergency response teams.

- The **Organizational PoC** list is sorted in alphabetical order by organization and by name.
- The **Computer Emergency Response Team** list is sorted in alphabetical order.

Abbreviations have been used in the Organization and Office columns. The following is a list of abbreviations used.

AFIWC	Air Force Information Warfare Center
AIA	Air Intelligence Agency
CDTD	Critical Defense Technology Division
CIA	Central Intelligence Agency
CIAC	Computer Incident Advisory Capability
CISA	C4I Integration Support Activity
CISS	Center for Information Systems Security
CIWE	Center for Information Warfare Excellence
CNA	Center for Naval Analyses
CNO N64	Chief of Naval Operations, Space and Electronic Combat Division
CPRGS	Commission on Protecting and Reducing Government Secrecy
CSIS	Center for Strategic and International Studies
CSSPAB	Computer Systems Security and Privacy Advisory Board
DARPA	Defense Advanced Research Projects Agency
DCI	Director, Central Intelligence
DHHS	Department of Health and Human Services
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DNA	Defense Nuclear Agency
DoC	Department of Commerce
DoE	Department of Energy
DoI	Department of Interior
DoJ	Department of Justice
DoS	Department of State
DoT	Department of Transportation
DoTreas	Department of the Treasury
DVA	Department of Veterans Affairs
EOP	Executive Office of the President
FACSPMF	Federal Agency Computer Security Program Managers Forum
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FIWC	Fleet Information Warfare Center
FRS	Federal Reserve System
GAO	Government Accounting Office
GPO	Government Printing Office
GSA	General Services Administration
HAC	House Appropriations Committee
HoR	House of Representatives
HQAF	Headquarters, Department of the Air Force
HQDA	Headquarters, Department of the Army
HQMC	Headquarters, Marine Corps
IDA	Institute for Defense Analyses
IIOO	INFOSEC Integration and Oversight Office
IITF	Information Infrastructure Task Force
IRM	Information Resources Management
IWB	Information Warfare Branch
JPSTC	Joint Program Office for Special Technical Countermeasures
JS	Joint Staff
LANL	Los Alamos National Laboratory
LIWA	Land Information Warfare Activity
LIWA	Land Information Warfare Activity
LLNL	Lawrence Livermore National Laboratory
NAS	National Academy of Sciences
NASA	National Aeronautics and Space Administration
NCIS	Naval Criminal Investigative Service
NDU	National Defense University
NEC	National Economic Council
NIMA	National Imagery and Mapping Agency
NIST	National Institute of Standards and Technology
NIWA	Naval Information Warfare Activity
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
NSC	National Security Council
NSTISSC	National Security Telecommunications and Information Systems Security
NTIA	National Telecommunications Information Administration
OASD(C3I)	Office of the Assistant Secretary of Defense (C3I)
ODCSOPS	Office of the Deputy Chief of Staff for Operations and Plans
OGC	Office of the General Council
OIS	Office of Information Security
OMB	Office of Management and Budget
OMNCS	Office of the Manager, National Communications System
ONA	Office of Net Assessment
OoSEC	Office of Security
OSD	Office of the Secretary of Defense
OSI	Office of Special Investigations
OSTP	Office of Science and Technology Policy
OTA	Office of Technology Assessment
OUSD(P)	Office of the Under Secretary of Defense (Policy)
OWTP	Office of Weaponry Technology and Proliferation
PNNL	Pacific Northwest National Laboratory
SAIC	Science Applications International Corporation
SEC	Securities Exchange Commission
SIF	Security Issues Forum

SNL	Sandia National Laboratory
STIC	Science and Technology Information Center
TNSO	Telecommunications and Networking Systems Operation
USA	United States Army
USAF	United States Air Force
USAWC	United States Army War College
USCG	United States Coast Guard
USDA	United States Department of Agriculture
USIA	United States Information Agency
USMC	United States Marine Corps
USN	United States Navy
USPS	United States Postal Service
USSPB	United States Security Policy Board
USSS	United States Secret Service
USSS	United States Secret Service

POINTS OF CONTACT: BY ORGANIZATION

Organization	Office	Name	Phone Number
CIA	OWTP	Chief, CDTD,	703-874-0394
CIA	OWTP	Chief, IWB,	703-874-0281
CNA		Federici, Gary, Mr.	703-824-2504
CPRGS		White, Mike, Mr.	202-776-8753
CSIS		Cilluffo, Frank, Mr.	202-775-3279
CSSPAB		Ware, Willis, Dr.	310-393-0411
DARPA		Lunt, Teresa, Ms.	703-696-4469
DCI		Benjamin, Jeffrey, Mr.	703-482-6811
DCI		Permann, Shelley,	703-482-2381
DHHS		Gignilliat, Bob, Mr.	202-690-7288
DHHS		Taylor, Alford, Mr.	301-443-1167
DHHS		Young, Frank, Dr.	301-443-1167
DIA		Lamb, Mike, Mr.	202-231-4094
DIA		Price, Glenn, Mr.	202-231-3992
DIA		Young, Stan, Mr.	202-373-4500
DIA		Yurechko, John, Mr.	202-373-8384
DISA		Smith, Carl, Mr.	703-607-6759
DISA		Weeks, Rebecca, LtCol	703-607-6096
DISA	CISS	League, Sara Jane, Ms.	703-681-7930
DISA	IIOO	Herrod, Chrisan, Ms.	703-607-6801
DISA	IIOO	Twomey, Tim, Mr.	703-681-7926
DoC		Balutis, Alan, Mr.	202-482-3490
DoC		Gibbon, Jerry, Mr.	202-482-3501
DoC		Hack, Ronald, Mr.	202-482-0120
DoC		Imber, George, Mr.	202-482-0873
DoC		Scott, Tom, Mr.	202-482-0694
DoC		Squier, James, Mr.	202-482-2855
DoC		Zetty, Tom, Mr.	202-482-3501
DoC	NIST	Roback, Ed, Mr.	301-975-3696
DoC	NTIA	Belote, Bill, Mr.	202-482-2473
DoC	NTIA	Gamble, Bill, Mr.	202-482-1850
DoC	NTIA	Parlow, Dick, Mr.	202-482-1850
DoD	JPO STC	Agudo, Mike, Dr.	540-653-6802
DoE		Davis, Mary Beth, Ms.	202-586-5002
DoE		Frampton, Brent, Mr.	202-586-9402
DoE		Przysucha, John, Mr.	301-903-4730
DoE		Rowlett, Tom, Mr.	301-903-3046
DoE		Wallace, Mary Ann, Ms.	301-903-3524
DoE		Wilcher, Larry, Mr.	202-903-5217

Organization	Office	Name	Phone Number
DoE	CIAC	Sparks, Sandra, Ms.	510-422-6856
DoE	LANL	Hunteman, William, Mr.	505-667-0096
DoE	LLNL	Mansur, Doug, Mr.	510-422-0896
DoE	ORNL	Jacobsen, Sharon, Ms.	615-574-0900
DoE	PNNL	Miles, D.R.,	509-372-4515
DoE	SNL	Sprauer, Patricia, Ms.	505-844-1555
DoI		Dolezal, Jim, Mr.	202-208-5002
DoI		Gordon, Gayle, Ms.	202-208-6194
DoJ		Charney, Scott, Mr.	202-514-1026
DoJ		Condon, Mary Ellen, Ms.	202-514-4292
DoJ		Shiveley, Wayne, Mr.	703-827-5110
DoJ		Skolochenko, Steve, Mr.	202-616-1162
DoJ		Stansell-Gamm, Martha, Ms.	202-616-0782
DoJ	FBI	Bryant, Robert, Mr.	202-324-3000
DoJ	FBI	Gallagher, Neil, Mr.	202-324-5740
DoJ	FBI	Geide, Ken, Mr.	202-324-8462
DoJ	FBI	Hughes, Dennis, Mr.	202-234-4974
DoJ	FBI	Perez, Bill, SSA	202-324-5514
DoJ	FBI	Ress, Richard, Mr.	202-324-9168
DoJ	IRM	Boster, Mark, Dr.	202-514-0507
DoS		Geisel, Hal, Mr.	202-647-2889
DoS		Johnson-Braun, Kim, Ms.	202-663-0346
DoS		Lake, Joseph, Mr.	202-647-2889
DoS		McClenaghan, Eliza, Ms.	202-607-2223
DoS		Osthaus, John, Mr.	202-647-2624
DoS		Romagnoli, Jules, Mr.	202-663-0019
DoT		Bussey, III, Jim, LCDR	202-366-9690
DoT		Correia, Nancy, Ms.	202-366-9691
DoT		Kane, Mike, Mr.	202-366-9715
DoT		Taylor, Eugene (Kip), Mr.	202-366-9201
DoT	USCG	Potter, Dave, CAPT	202-267-2766
DoTreas		Chou, Wushow	202-622-1200
DoTreas		Ferris, Marty, Mr.	202-622-2064
DoTreas		Flyzik, Jim, Mr.	202-622-1592
DoTreas		Sullivan, Jane, Ms.	202-622-1599
DoTreas		Wunderlich, Bill, Mr.	202-622-1553
DoTreas	OoSec	Riley, Rick, Mr.	202-622-1120
DoTreas	USSS	Riley, Mary, Ms.	202-435-7823
DoTreas	USSS	Robeck, Mike, Mr.	202-435-5266
DVA		Boyd, Howard, Mr.	202-273-5510
DVA		Lalley, Frank, Mr.	202-565-4311
EOP	NEC	Kalil, Tom, Mr.	202-456-2802

Organization	Office	Name	Phone Number
EOP	NSC	Appel, Ed, Mr.	202-456-9341
EOP	NSC	Beers, Randy, Mr.	202-456-9341
EOP	NSC	Sestak, Joe, CAPT	202-456-9191
EOP	OMB	Brower, Paul, Dr.	202-395-4800
EOP	OMB	McConnell, Bruce, Mr.	202-395-3785
EOP	OMB	Schlarman, Glenn, Mr.	202-395-3785
EOP	OMB	Springer, Ed, Mr.	202-395-3562
EOP	OSTP	Fuhrman, Tom, Mr.	202-456-6057
EOP	OSTP	Johnson, Lee,	202-456-6060
FACSPMF		Pitcher, Sadie, Ms.	202-482-0605
FCC		Kolly, Roy, Mr.	202-418-1150
FCC		Neumann, Herb, Mr.	202-418-2341
FCC		van Doorn, Arlan, Mr.	202-418-1100
FEMA		Donovan, William, Mr.	202-646-3542
FEMA		Green, Dennis, Mr.	202-646-3470
FEMA		Massa, Joe, Mr.	202-646-3083
FRS		Buckley, Ken, Mr.	202-452-3646
FRS		Parrish, John, Mr.	202-452-2224
FRS		Romero, Ray, Mr.	202-452-2832
GAO		Boland, F. Kevin, Mr.	202-512-6623
GAO		Hinton, Buthc, Mr.	202-512-4300
GAO	IRM	Brock, Jack, Mr.	202-512-6240
GPO		Russell, Judith, Ms.	202-512-1265
GSA		Brignall, Bruce, Mr.	703-883-3358
GSA		Flynn, George, Mr.	202-501-0843
GSA		Savoy, Diane, Ms.	202-219-3075
GSA		Venneberg, Don, Mr.	202-501-1000
GSA		Woods, Bob, Mr.	703-285-1020
GSA	OIS	Burke, Tom, Mr.	202-708-7000
GSA	OIS	Specht, John, Mr.	202-708-7000
HoR		Baker, T. Keith, Mr.	703-351-2567
HoR		Haurer, Carroll, Mr.	703-351-2567
HoR		Mullenhoff, Paul, Mr.	703-351-2567
HoR	HAC	Lilly, Scott, Mr.	202-225-3481
IDA		Anthony, Robert, Dr.	703-845-2388
IDA		Barlow, Bill, Mr.	703-845-2465
IDA		Mayfield, Terry, Mr.	703-845-6602
IDA		Shay III, John, Dr.	703-845-2418
IITF		Barrett, Yevette, Ms.	202-482-1835
IITF	SIF	Huth, Virginia, Ms.	202-395-6929
JS		Sharp, Walter, LtCol	703-697-1137
JS	J2	Thompson, Marcum, LtCol	703-614-4921

Organization	Office	Name	Phone Number
JS	J6K	Davis, Kris, LCDR	703-693-4578
JS	J6K	Gorrie, Bob, LTC (P)	703-614-5990
JS	J6K	Gravell, Bill, CAPT	703-614-2918
JS	J6K	Luzwick, Perry, Major	703-697-8896
JS	J6K	Spano, Steve, Lt Col (S)	703-697-1199
JS	J6K	Walsh, Buzz, Major	703-614-2403
JS	NDU	Alger, John, Dr.	202-685-2249
JS	NDU	Barriteau, Brad, Mr.	202-685-2246
JS	NDU	Casey, Richard, Lt. Col.	202-685-2248
JS	NDU	Czerwinski, Tom, Mr.	202-685-2245
JS	NDU	Ducharme, Lee, CDR	202-685-2248
JS	NDU	Giessler, Fred, Dr.	202-685-2258
JS	NDU	Kuehl, Dan, Dr.	202-685-2257
NAS	NRC	Blumenthal, Majorie, Ms.	202-334-2605
NAS	NRC	Lin, Herbert, Mr.	202-334-2605
NASA		Borsi, Mark, Mr.	202-358-0118
NASA		Carr, Rick, Mr.	202-358-2309
NASA		Force, Charles, Mr.	202-358-2020
NASA		Rice, Russel, Mr.	202-358-1790
NASA		Sigust, Art, Mr.	202-358-4787
NASA		Sutton, Jeffrey, Mr.	202-358-2800
NASA		Toraine, Brad, Mr.	301-286-6990
NCIS		Parsons, Mat, SA	202-433-9293
NIST		Grance, Tim, Mr.	301-975-4242
NIST		Katzke, Stuart, Dr.	301-975-2934
NIST		Smid, Miles, Mr.	301-975-2938
NRC		Brady, Raymond, Mr.	301-415-8100
NRC		Cranford, Gerald, Mr.	301-415-7585
NRC		Kellum, Tom, Mr.	301-415-7429
NRC		Kruzic, Pam, Ms.	301-415-7575
NRC		Messenger, George, Mr.	301-415-7546
NRC		Norry, Patricia, Ms.	301-415-7443
NSA		Baggett, Charlie, Mr.	410-684-7087
NSA		Brooks, Clint, Dr.	301-688-4260
NSA		Green, Mike, Mr.	410-859-6884
NSA		Lee, Ronald, Mr.	301-688-6705
NSA		Snow, Brian, Mr.	301-688-8112
NSA		Spencer, John, Mr.	301-688-5131
NSA	CIWE	Larson, Gerald, Mr.	301-688-5131
NSA	NSTISSC	Rothstein, George, Mr.	410-859-6805
OMNCS		Caputo, Chuck, Mr.	703-607-6220
OMNCS		Centra, Mark, Mr.	703-607-6183

Organization	Office	Name	Phone Number
OMNCS		Fletcher, Jim, LTC	703-607-6207
OMNCS		Fountain, Diane, Ms.	703-607-6101
OMNCS	N53	Herr, Fred, Mr.	703-607-6184
OMNCS	N53	Kerr, Jim, Mr.	703-607-6133
OSD	CISA	Miner, Barry, COL	703-695-1081
OSD	OASD(C3I)	Anderson, Bob, Mr.	703-697-5508
OSD	OASD(C3I)	Blackburn, Greg, CAPT	703-693-2157
OSD	OASD(C3I)	Callahan, Roger, Mr.	703-695-8705
OSD	OASD(C3I)	Frizzell, Joe, Dr.	703-697-5508
OSD	OASD(C3I)	Hill, Martin, Mr.	703-614-0624
OSD	OASD(C3I)	O'Neill, Dick, CAPT	703-694-0625
OSD	OASD(C3I)	Soos, James, Dr.	703-695-2396
OSD	OGC	DeRosa, Mary, Ms.	703-695-6710
OSD	ONA	FitzSimonds, Jim, CAPT	703-697-1312
OSD	ONA	Miller, Chuck, COL	703-697-1312
OSD	ONA	Rowell, Scott, COL	703-697-1312
OSD	ONA	van Tol, Jan, CDR	703-697-1312
OSD	OUSD(P)	Dryden, Sheila, Ms.	703-681-9741
OSD	OUSD(P)	Greene, Brent, Mr.	703-614-2616
OSD	OUSD(P)	Guissanie, Gus, Mr.	703-681-5650
OSD	OUSD(P)	Turner, Glenda, Ms.	703-681-5650
SAIC	DoE	Huggin, Ben, Mr.	301-353-8386
SAIC	TNSO	Devost, Matthew, Mr.	703-287-7604
SAIC	TNSO	Hutchins, Rosemary, Ms.	703-734-5832
SAIC	TNSO	Rankin, Bob, Mr.	703-556-7008
SAIC	TNSO	Tompkins, Fred, Mr.	703-821-4385
SAIC	TNSO	Ziegler, Bernie, Mr.	703-790-7452
SEC		Bartell, Mike, Mr.	202-942-8802
SEC		Butler, Wilson, Mr.	202-942-8938
USA	HQDA	Brown, Mike, COL	703-697-1474
USA	HQDA	Harrison, Donal, Mr.	703-697-0612
USA	HQDA	Loranger, Phil, Mr.	703-693-3344
USA	LIWA	Hudson, Tom, LTC	703-706-2263
USA	LIWA	Stevens, Halbert, COL	703-706-1791
USA	LIWA	Virtes, Bob, LTC	703-706-2262
USA	ODCSOPS	Jones, Craig, LTC	703-697-1119
USA	STIC	Burnett, Kay, Ms.	804-980-7884
USA	USAWC	Gooden, R. Thomas, Dr.	717-245-4530
USAF		Bush, Henry, Mr.	315-330-3042
USAF		Goessman, , Mr.	618-256-4450
USAF		Pirog, John, Mr.	315-330-7990
USAF		Rhoades, Walter, Lt Col	803-668-5310

Organization	Office	Name	Phone Number
USAF		Williams, Lee, Capt	617-271-7358
USAF	AFIWC	Ramirez, Fred, Mr.	800-854-0187
USAF	AFIWC	Rodriguez, Feliciano, Mr.	210-977-3990
USAF	AIA	Ramirez, Maria, Ms.	210-977-2465
USAF	HQAF	Blunden, , Lt. Col	703-695-7817
USAF	HQAF	Fiedler, George, Col	703-697-2108
USAF	HQAF	Lieberherr, , Col	703-697-9390
USAF	HQAF	Mullins, Mark, Major	703-697-2108
USAF	HQAF	Wheeler, Greg, Colonel	703-697-8044
USAF	HQAF	Zernial, Ernie, Lt Col	703-697-2108
USAF	OSI	DeMaggio, John, Mr.	202-404-1686
USAF	OSI	Schmidt, Howard, Mr.	202-404-1686
USCG		Chiswell, Ben, CAPT	202-267-6856
USCG		Grimes, Mike, CDR	202-267-1269
USCG		Inman, Mike, LCDR	202-267-6020
USCG		Mead, Mike, CAPT	202-267-2576
USCG		Patrick, Jim, Lt.	202-267-6598
USDA		Boger, Brenda, Ms.	202-720-8025
USDA		Hardesty, Don, Mr.	202-720-3152
USIA		Barnett, Gary, Mr.	202-619-6509
USMC	HQMC	Areola, Dave, CAPT	703-614-4220
USMC	HQMC	Snyder, Marshall, LtCol	703-693-3136
USMC	HQMC	Wiedower, Robert, Major	703-614-4221
USN	CNO N64	Burnette, Gary, LCDR	703-695-0951
USN	CNO N64	Caldarella, Rocco, CAPT	703-695-0951
USN	CNO N64	Galik, D., CDR	703-697-7755
USN	CNON64	Sprout, Rick, Major	703-697-7755
USN	FIWC	Barrett, Gary, CAPT	804-864-8840
USN	NIWA	Handel, Tom, Mr.	301-669-3090
USPS		Patterson, Tim, Mr.	919-501-9074
USSPB		Knauf, Dan, Mr.	703-602-9974
USSPB		LaBarre, Vicki, Ms.	703-602-9993

POINTS OF CONTACT: BY NAME

Name	Organization	Office	Phone Number
Agudo, Mike, Dr.	DoD	JPO STC	540-653-6802
Alger, John, Dr.	JS	NDU	202-685-2249
Anderson, Bob, Mr.	OSD	OASD(C3I)	703-697-5508
Anthony, Robert, Dr.	IDA		703-845-2388
Appel, Ed, Mr.	EOP	NSC	202-456-9341
Areola, Dave, CAPT	USMC	HQMC	703-614-4220
Baggett, Charlie, Mr.	NSA		410-684-7087
Baker, T. Keith, Mr.	HoR		703-351-2567
Balutis, Alan, Mr.	DoC		202-482-3490
Barlow, Bill, Mr.	IDA		703-845-2465
Barnett, Gary, Mr.	USIA		202-619-6509
Barrett, Gary, CAPT	USN	FIWC	804-864-8840
Barrett, Yevette, Ms.	IITF		202-482-1835
Barriteau, Brad, Mr.	JS	NDU	202-685-2246
Bartell, Mike, Mr.	SEC		202-942-8802
Beers, Randy, Mr.	EOP	NSC	202-456-9341
Belote, Bill, Mr.	DoC	NTIA	202-482-2473
Benjamin, Jeffrey, Mr.	DCI		703-482-6811
Blackburn, Greg, CAPT	OSD	OASD(C3I)	703-693-2157
Blumenthal, Majorie, Ms.	NAS	NRC	202-334-2605
Blunden, , Lt. Col	USAF	HQAF	703-695-7817
Boger, Brenda, Ms.	USDA		202-720-8025
Boland, F. Kevin, Mr.	GAO		202-512-6623
Borsi, Mark, Mr.	NASA		202-358-0118
Boster, Mark, Dr.	DoJ	IRM	202-514-0507
Boyd, Howard, Mr.	DVA		202-273-5510
Brady, Raymond, Mr.	NRC		301-415-8100
Brignall, Bruce, Mr.	GSA		703-883-3358
Brock, Jack, Mr.	GAO	IRM	202-512-6240
Brooks, Clint, Dr.	NSA		301-688-4260
Brower, Paul, Dr.	EOP	OMB	202-395-4800
Brown, Mike, COL	USA	HQDA	703-697-1474
Bryant, Robert, Mr.	DoJ	FBI	202-324-3000
Buckley, Ken, Mr.	FRS		202-452-3646
Burke, Tom, Mr.	GSA	OIS	202-708-7000
Burnett, Kay, Ms.	USA	STIC	804-980-7884
Burnette, Gary, LCDR	USN	CNO N64	703-695-0951
Bush, Henry, Mr.	USAF		315-330-3042
Bussey, III, Jim, LCDR	DoT		202-366-9690

Name	Organization	Office	Phone Number
Butler, Wilson, Mr.	SEC		202-942-8938
Caldarella, Rocco, CAPT	USN	CNO N64	703-695-0951
Callahan, Roger, Mr.	OSD	OASD(C3I)	703-695-8705
Caputo, Chuck, Mr.	OMNCS		703-607-6220
Carr, Rick, Mr.	NASA		202-358-2309
Casey, Richard, Lt. Col.	JS	NDU	202-685-2248
Centra, Mark, Mr.	OMNCS		703-607-6183
Charney, Scott, Mr.	DoJ		202-514-1026
Chief, CDTD,	CIA	OWTP	703-874-0394
Chief, IWB,	CIA	OWTP	703-874-0281
Chiswell, Ben, CAPT	USCG		202-267-6856
Chou, Wushow	DoTreas		202-622-1200
Cilluffo, Frank, Mr.	CSIS		202-775-3279
Condon, Mary Ellen, Ms.	DoJ		202-514-4292
Correia, Nancy, Ms.	DoT		202-366-9691
Cranford, Gerald, Mr.	NRC		301-415-7585
Czerwinski, Tom, Mr.	JS	NDU	202-685-2245
Davis, Kris, LCDR	JS	J6K	703-693-4578
Davis, Mary Beth, Ms.	DoE		202-586-5002
DeMaggio, John, Mr.	USAF	OSI	202-404-1686
DeRosa, Mary, Ms.	OSD	OGC	703-695-6710
Devost, Matthew, Mr.	SAIC	TNSO	703-287-7604
Dolezal, Jim, Mr.	DoI		202-208-5002
Donovan, William, Mr.	FEMA		202-646-3542
Dryden, Sheila, Ms.	OSD	OUSD(P)	703-681-9741
Ducharme, Lee, CDR	JS	NDU	202-685-2248
Federici, Gary, Mr.	CNA		703-824-2504
Ferris, Marty, Mr.	DoTreas		202-622-2064
Fiedler, George, Col	USAF	HQAF	703-697-2108
FitzSimonds, Jim, CAPT	OSD	ONA	703-697-1312
Fletcher, Jim, LTC	OMNCS		703-607-6207
Flynn, George, Mr.	GSA		202-501-0843
Flyzik, Jim, Mr.	DoTreas		202-622-1592
Force, Charles, Mr.	NASA		202-358-2020
Fountain, Diane, Ms.	OMNCS		703-607-6101
Frampton, Brent, Mr.	DoE		202-586-9402
Frizzell, Joe, Dr.	OSD	OASD(C3I)	703-697-5508
Fuhrman, Tom, Mr.	EOP	OSTP	202-456-6057
Galik, D., CDR	USN	CNO N64	703-697-7755
Gallagher, Neil, Mr.	DoJ	FBI	202-324-5740
Gamble, Bill, Mr.	DoC	NTIA	202-482-1850
Geide, Ken, Mr.	DoJ	FBI	202-324-8462

Name	Organization	Office	Phone Number
Geisel, Hal, Mr.	DoS		202-647-2889
Gibbon, Jerry, Mr.	DoC		202-482-3501
Giessler, Fred, Dr.	JS	NDU	202-685-2258
Gignilliat, Bob, Mr.	DHHS		202-690-7288
Goessman, , Mr.	USAF		618-256-4450
Gooden, R. Thomas, Dr.	USA	USAWC	717-245-4530
Gordon, Gayle, Ms.	DoI		202-208-6194
Gorrie, Bob, LTC (P)	JS	J6K	703-614-5990
Grance, Tim, Mr.	NIST		301-975-4242
Gravell, Bill, CAPT	JS	J6K	703-614-2918
Green, Dennis, Mr.	FEMA		202-646-3470
Green, Mike, Mr.	NSA		410-859-6884
Greene, Brent, Mr.	OSD	OUSD(P)	703-614-2616
Grimes, Mike, CDR	USCG		202-267-1269
Guissanie, Gus, Mr.	OSD	OUSD(P)	703-681-5650
Hack, Ronald, Mr.	DoC		202-482-0120
Handel, Tom, Mr.	USN	NIWA	301-669-3090
Hardesty, Don, Mr.	USDA		202-720-3152
Harrison, Donal, Mr.	USA	HQDA	703-697-0612
Haurer, Carroll, Mr.	HoR		703-351-2567
Herr, Fred, Mr.	OMNCS	N53	703-607-6184
Herrod, Chrisan, Ms.	DISA	IIOO	703-607-6801
Hill, Martin, Mr.	OSD	OASD(C3I)	703-614-0624
Hinton, Buthc, Mr.	GAO		202-512-4300
Hudson, Tom, LTC	USA	LIWA	703-706-2263
Huggin, Ben, Mr.	SAIC	DoE	301-353-8386
Hughes, Dennis, Mr.	DoJ	FBI	202-234-4974
Hunteman, William, Mr.	DoE	LANL	505-667-0096
Hutchins, Rosemary, Ms.	SAIC	TNSO	703-734-5832
Huth, Virginia, Ms.	IITF	SIF	202-395-6929
Imber, George, Mr.	DoC		202-482-0873
Inman, Mike, LCDR	USCG		202-267-6020
Jacobsen, Sharon, Ms.	DoE	ORNL	615-574-0900
Johnson, Lee,	EOP	OSTP	202-456-6060
Johnson-Braun, Kim, Ms.	DoS		202-663-0346
Jones, Craig, LTC	USA	ODCSOPS	703-697-1119
Kalil, Tom, Mr.	EOP	NEC	202-456-2802
Kane, Mike, Mr.	DoT		202-366-9715
Katzke, Stuart, Dr.	NIST		301-975-2934
Kellum, Tom, Mr.	NRC		301-415-7429
Kerr, Jim, Mr.	OMNCS	N53	703-607-6133
Knauf, Dan, Mr.	USSPB		703-602-9974

Name	Organization	Office	Phone Number
Kolly, Roy, Mr.	FCC		202-418-1150
Kruzic, Pam, Ms.	NRC		301-415-7575
Kuehl, Dan, Dr.	JS	NDU	202-685-2257
LaBarre, Vicki, Ms.	USSPB		703-602-9993
Lake, Joseph, Mr.	DoS		202-647-2889
Lalley, Frank, Mr.	DVA		202-565-4311
Lamb, Mike, Mr.	DIA		202-231-4094
Larson, Gerald, Mr.	NSA	CIWE	301-688-5131
League, Sara Jane, Ms.	DISA	CISS	703-681-7930
Lee, Ronald, Mr.	NSA		301-688-6705
Lieberherr, , Col	USAF	HQAF	703-697-9390
Lilly, Scott, Mr.	HoR	HAC	202-225-3481
Lin, Herbert, Mr.	NAS	NRC	202-334-2605
Loranger, Phil, Mr.	USA	HQDA	703-693-3344
Lunt, Teresa, Ms.	DARPA		703-696-4469
Luzwick, Perry, Major	JS	J6K	703-697-8896
Mansur, Doug, Mr.	DoE	LLNL	510-422-0896
Massa, Joe, Mr.	FEMA		202-646-3083
Mayfield, Terry, Mr.	IDA		703-845-6602
McClenaghan, Eliza, Ms.	DoS		202-607-2223
McConnell, Bruce, Mr.	EOP	OMB	202-395-3785
Mead, Mike, CAPT	USCG		202-267-2576
Messenger, George, Mr.	NRC		301-415-7546
Miles, D.R.,	DoE	PNNL	509-372-4515
Miller, Chuck, COL	OSD	ONA	703-697-1312
Miner, Barry, COL	OSD	CISA	703-695-1081
Mullenhoff, Paul, Mr.	HoR		703-351-2567
Mullins, Mark, Major	USAF	HQAF	703-697-2108
Neumann, Herb, Mr.	FCC		202-418-2341
Norry, Patricia, Ms.	NRC		301-415-7443
O'Neill, Dick, CAPT	OSD	OASD(C3I)	703-694-0625
Osthaus, John, Mr.	DoS		202-647-2624
Parlow, Dick, Mr.	DoC	NTIA	202-482-1850
Parrish, John, Mr.	FRS		202-452-2224
Parsons, Mat, SA	NCIS		202-433-9293
Patrick, Jim, Lt.	USCG		202-267-6598
Patterson, Tim, Mr.	USPS		919-501-9074
Perez, Bill, SSA	DoJ	FBI	202-324-5514
Permann, Shelley,	DCI		703-482-2381
Pirog, John, Mr.	USAF		315-330-7990
Pitcher, Sadie, Ms.	FACSPMF		202-482-0605
Potter, Dave, CAPT	DoT	USCG	202-267-2766

Name	Organization	Office	Phone Number
Price, Glenn, Mr.	DIA		202-231-3992
Przysucha, John, Mr.	DoE		301-903-4730
Ramirez, Fred, Mr.	USAF	AFIWC	800-854-0187
Ramirez, Maria, Ms.	USAF	AIA	210-977-2465
Rankin, Bob, Mr.	SAIC	TNSO	703-556-7008
Ress, Richard, Mr.	DoJ	FBI	202-324-9168
Rhoades, Walter, Lt Col	USAF		803-668-5310
Rice, Russel, Mr.	NASA		202-358-1790
Riley, Mary, Ms.	DoTreas	USSS	202-435-7823
Riley, Rick, Mr.	DoTreas	OoSec	202-622-1120
Roback, Ed, Mr.	DoC	NIST	301-975-3696
Robeck, Mike, Mr.	DoTreas	USSS	202-435-5266
Rodriguez, Feliciano, Mr.	USAF	AFIWC	210-977-3990
Romagnoli, Jules, Mr.	DoS		202-663-0019
Romero, Ray, Mr.	FRS		202-452-2832
Rothstein, George, Mr.	NSA	NSTISSC	410-859-6805
Rowell, Scott, COL	OSD	ONA	703-697-1312
Rowlett, Tom, Mr.	DoE		301-903-3046
Russell, Judith, Ms.	GPO		202-512-1265
Savoy, Diane, Ms.	GSA		202-219-3075
Schlarman, Glenn, Mr.	EOP	OMB	202-395-3785
Schmidt, Howard, Mr.	USAF	OSI	202-404-1686
Scott, Tom, Mr.	DoC		202-482-0694
Sestak, Joe, CAPT	EOP	NSC	202-456-9191
Sharp, Walter, LtCol	JS		703-697-1137
Shay III, John, Dr.	IDA		703-845-2418
Shiveley, Wayne, Mr.	DoJ		703-827-5110
Sigust, Art, Mr.	NASA		202-358-4787
Skolochenko, Steve, Mr.	DoJ		202-616-1162
Smid, Miles, Mr.	NIST		301-975-2938
Smith, Carl, Mr.	DISA		703-607-6759
Snow, Brian, Mr.	NSA		301-688-8112
Snyder, Marshall, LtCol	USMC	HQMC	703-693-3136
Soos, James, Dr.	OSD	OASD(C3I)	703-695-2396
Spano, Steve, Lt Col (S)	JS	J6K	703-697-1199
Sparks, Sandra, Ms.	DoE	CIAC	510-422-6856
Specht, John, Mr.	GSA	OIS	202-708-7000
Spencer, John, Mr.	NSA		301-688-5131
Sprauer, Patricia, Ms.	DoE	SNL	505-844-1555
Springer, Ed, Mr.	EOP	OMB	202-395-3562
Sprout, Rick, Major	USN	CNON64	703-697-7755
Squier, James, Mr.	DoC		202-482-2855

Name	Organization	Office	Phone Number
Stansell-Gamm, Martha, Ms.	DoJ		202-616-0782
Stevens, Halbert, COL	USA	LIWA	703-706-1791
Sullivan, Jane, Ms.	DoTreas		202-622-1599
Sutton, Jeffrey, Mr.	NASA		202-358-2800
Taylor, Alford, Mr.	DHHS		301-443-1167
Taylor, Eugene (Kip), Mr.	DoT		202-366-9201
Thompson, Marcum, LtCol	JS	J2	703-614-4921
Tompkins, Fred, Mr.	SAIC	TNSO	703-821-4385
Toraine, Brad, Mr.	NASA		301-286-6990
Turner, Glenda, Ms.	OSD	OUSD(P)	703-681-5650
Twomey, Tim, Mr.	DISA	IIOO	703-681-7926
van Doorn, Arlan, Mr.	FCC		202-418-1100
van Tol, Jan, CDR	OSD	ONA	703-697-1312
Venneberg, Don, Mr.	GSA		202-501-1000
Virtes, Bob, LTC	USA	LIWA	703-706-2262
Wallace, Mary Ann, Ms.	DoE		301-903-3524
Walsh, Buzz, Major	JS	J6K	703-614-2403
Ware, Willis, Dr.	CSSPAB		310-393-0411
Weeks, Rebecca, LtCol	DISA		703-607-6096
Wheeler, Greg, Colonel	USAF	HQAF	703-697-8044
White, Mike, Mr.	CPRGS		202-776-8753
Wiedower, Robert, Major	USMC	HQMC	703-614-4221
Wilcher, Larry, Mr.	DoE		202-903-5217
Williams, Lee, Capt	USAF		617-271-7358
Woods, Bob, Mr.	GSA		703-285-1020
Wunderlich, Bill, Mr.	DoTreas		202-622-1553
Young, Frank, Dr.	DHHS		301-443-1167
Young, Stan, Mr.	DIA		202-373-4500
Yurechko, John, Mr.	DIA		202-373-8384
Zernial, Ernie, Lt Col	USAF	HQAF	703-697-2108
Zetty, Tom, Mr.	DoC		202-482-3501
Ziegler, Bernie, Mr.	SAIC	TNSO	703-790-7452

COMPUTER EMERGENCY RESPONSE TEAMS

Response Team	Constituency	Email/ WWW URL	Phone #s
Advanced Network Services, INC (ANS)	ANS Customers	anscert@ans.net http://www.ans.net	313-677-7350 313-677-7333 emergency 313-677-7310 fax
Air Force CERT (AFCERT)	Air Force	afcert@afcert.csap.af.mil	210-977-3157 800-854-0187 pager 210-977-4567 fax
Apple Computer	Apple Computer	lsefton@apple.com	408-974-5594 408-974-4754 fax
Australian CERT (AUSCERT)	Australia	auscert@auscert.org.au http://www.auscert.org.au	61-7-3365-4417 61-7-3365-4477
Bellcore	Bellcore	sb3@cc.bellcore.com	908-758-5860 908-758-4504 fax
Boeing CERT (BCERT)	Boeing	compsec@maple.a1.boeing.com	206-657-9405 206-655-2222 emergency 206-657-9477 fax
BSI/GISA	German Government	fwf@bsi.de http://www.cert.dfn.de/eng	49-228-9582-248 49-228-9852-444 emergency 49-228-9582-400 fax
CCTA	UK Government and Agencies	cbaxter.esb.ccta@gnet.gov.uk	44-0171-824-4101/2 44-0171-305-3178 fax
CERT Coordination Center	UNIX, Internet Research	cert@cert.org http://www.cert.org	412-268-7090 412-268-6989 fax
CERT-IT	Italian Internet Sites	cert-it@dsi.unimi.it	39-2-5500-391 39-2-5500-392 emergency 39-2-5500-394 fax
CERT-NL	SURFnet Sites	cert-nl@surfnet.nl http://www.nic.surfnet.nl/surfnet/security/cert-nl.html	31-30-305-305 31-30-305-329 fax
Cisco Systems	Cisco Systems	karyn@cisco.com	408-526-5638 408-526-5420 fax
DEC SSRT	Digital Equipment Corp and Customers	rich.boren@cxo.mts.dec.com	800-354-9000 800-208-7940 emergency 901-761-6792 fax
Defence Research Agency, Malvern	Defense Research Agency	shore@ajax.dra.hmg.gb	44-01684-895425 44-01684-896113 fax
DFN CERT	Germany	dfncert@cert.dfn.de	49-40-54-715-262 49-40-54-715-241 fax
DISA	MILNET	scc@cc.ims.disa.mil	800-365-3642 703-692-5071 fax
DoD ASSIST	DoD Interest Systems	assist@assist.mil	800-357-4231 703-607-4735 fax
DOE CIAC	Department of Energy	ciac@llnl.gov http://ciac.llnl.gov	510-422-8193 510-423-8002 fax
DOW USA	DOW	whstewart@dow.com	517-636-8738 517-638-7705 fax
EDS	EDS and Customers	jcutle01@novell.trts01.eds.com	313-265-7514 313-265-3432 fax

Response Team	Constituency	Email/ WWW URL	Phone #s
FIRST	Forum of Incident Response and Security Teams	first-sec@first.org http://csrc.ncsl.nist.gov/first/	301-975-3359
General Electric	GE Businesses	sandstrom@gies.ges.com	301-340-4848 301-340-4059 fax
Goddard Space Flight Center	Goddard SPC	hmiddleton@gsfcmai.nasa.gov	301-286-7233 301-286-2923 fax
Goldman, Sachs and Company	Goldman, Sachs offices worldwide	safdas@gsco.com	212-357-1880 800-SKY-PAGE (1632254)
Hewlett Packard	All HP-UX Customers	security-alert@hp.com	
Israeli Academic Network	Israeli University users	cert-1@vm.tau.ac.il	972-3-6408309 972-3-6409118 fax
JANET CERT	All JANET networks	cert@cert.ja.net	44-01235-822-302 44-01235-822-898 fax
JP Morgan	JP Morgan employees and consultants		212-235-5010
MCI	Corporate System Security	6722867@mcimail.com	719-535-6932 800-SKY-8888 (190-2130) 719-535-1220 fax
Micro-BIT Virus Center	Anyone	ry15@uni-karlsruhe.de	49-721-376422 49-171-5251685 emergency 49-721-32550 fax
Motorola CERT	Motorola	mcert@mot.com	847-576-1616 847-576-0669 emergency 847-538-2153 fax
NASA (Ames Research Center)	Ames Research Center	hwalter@nas.nasa.gov	415-604-3402 415-604-4377 fax
NASIRC	NASA and International Aerospace community	nasirc@nasirc.nasa.gov http://nasirc.nasa.gov/NASIRC_home.html	800-762-7472 800-SKY-PAGE (2023056) 301-441-1853 fax
NAVCIRT	U.S. Navy	ldrich@fiwc.navy.mil http://infosec.nosc.mil/navcirt.html	804-464-8832 800-SKY-PAGE (5294117)
NIST/CSRC	National Institute of Standards and Tech.	jwack@nist.gov http://cs-www.ncsl.nist.gov	301-975-3359 301-948-0279 fax
NORDUnet	NORDUnet	ber@sunet.se	46-8-790-6513 46-8-24-11-79 fax
Northwestern University	Northwestern Faculty/Staff/Stude nts	r-safian@nwu.edu http://grumpy.acns.nwu.edu/nu-cert	847-491-4056 847-491-3824 fax
Penn State University	Penn State Faculty/Staff/Stude nts	krk5@psu.edu	814-863-9533 814-863-4375 emergency 814-865-3082 fax
Purdue CERT	Purdue University	pcert@cs.purdue.edu http://www.cs.purdue.edu/pcert/pcert.html	317-494-7844 317-494-6440 fax

Response Team	Constituency	Email/ WWW URL	Phone #s
Renater	Minister of Research and Education	morel@urec.fr	33-1-44-27-26-12 33-1-44-27-26-13 fax
SBACERT	Small Businesses Nationwide (US)	hfb@oirm.sba.gov	202-205-6708 202205-7064 fax
Silicon Graphics, Inc	Silicon Graphics User Community	security-alert@sgi.com	415-390-1237 415-390-6236 fax
Stanford University NST	Stanford University Faculty/Staff/Students	security@stanford.edu http://www.stanford.edu/~security/	415-723-2911 415-725-1548 fax
SUN Microsystems	SUN Customers	mark.graff@sun.com	415-786-5274 415-786-7994 fax
SWITCH	Swiss Universities and Government	cert-staff@switch.ch http://www.switch.ch/switch/cert	41-1-268-1518 41-1-760-2137 emergency 41-1-268-1568 fax
TRW Inc.	TRW Network and System Administrators	zorn@gumby.sp.trw.com	310-812-1839 310-813-4621 fax
U.S. Sprint	SprintNet (X.25) and Sprint Link (TCP/IP)	steve.matthews@sprint.sprint.com	703-904-2406 703-904-2708 fax
UCERT	UNISYS Users	garb@po3.bb.unisys.com	215-986-4038 215-330-2316 pager 215-986-4409 fax
Veterans Health Administration IRT	Veteran’s Health Administration	frank.marino@forum.va.gov http://www.va.gov	304-263-0811 (4062) 304-263-4748 emergency
Westinghouse Electric Corp.	Westinghouse Corp	nicholson.m%wec@dialcom.tymnet.com	412-642-3097 412-642-3871 fax

This page intentionally left blank.